中華人民共和國澳門特別行政區
Região Administrativa Especial de Macau da República Popular da China

澳門警學

Revista das Ciências Policiais de Macau

第六期 | 2024年 9月

- 電信網絡詐騙犯罪的演變分析與防控措施
- 電信網絡詐騙關聯犯罪治理研究——以幫信犯罪為視角
- 澳門保安範疇智慧雲警務數據治理的現狀分析及改善意見

ISSN 2789-9942

澳門保安部隊及保安部門
Forças e Serviços de Segurança de Macau

澳門警學

第六期
2024 年 9 月

本期《澳門警學》

目錄

特約

偵查研究

公共安全

科技強警

Contents

Invited Articles

Investigative Research

Public Security

Technology Police

電信網絡詐騙犯罪的演變分析與防控措施

牛驚雷、王豔紅 *

摘要：打擊防範電信網絡詐騙犯罪是一項長期工作，電信網絡詐騙活動不會隨着緬北電詐園區的瓦解而收斂，反而詐騙行為會借助新的技術手段形成新的演化。建立有效的防控體系，推動社會共治對於保障人民安居樂業，增強人民群眾獲得感、幸福感、安全感極為重要。電信網絡詐騙犯罪防控體系的建設要以電信網絡詐騙犯罪行為的底層邏輯為目標，根據電信網絡詐騙犯罪信息不對稱的運行機理，從信息不對稱產生的環節入手，全面揭示信息不對稱產生根源，由此構建有針對性的防控措施，才能有效提高反詐成效。

關鍵詞：電信網絡詐騙犯罪　防控　信息不對稱　演變

Analysis of the Evolution of Telecom Network Fraud Crimes and Prevention and Control Measures

Niu Jinglei; Wang Yanhong

Abstract: Combating and preventing telecom network fraud crimes is a long-term task. Telecom network fraud activities do not diminish with the collapse of the telecom fraud park in northern Myanmar; instead, fraud activities evolve through the adoption of new technological means. Establishing an effective prevention and control system and promoting social co-governance are crucial for ensuring people's well-being and enhancing their sense of gain, happiness, and security. The construction of a prevention and control system for telecom network fraud crimes should target the underlying logic of these crimes. Through the operational mechanism of information asymmetry in telecom network fraud crimes and identifying their root causes from the links where information asymmetry arises, targeted prevention and control measures can be developed to significantly improve anti-fraud effectiveness.

Keywords: Telecom Network Fraud Crimes; Prevention and Control; Information Asymmetry; Evolution

* 牛驚雷，中國人民警察大學偵查學院副教授、中國人民警察大學新型犯罪防控研究中心研究員，博士。研究方向：公共管理和社會治理。

* 王豔紅，中國人民警察大學偵查學院副教授、中國人民警察大學新型犯罪防控研究中心研究員，碩士。研究方向：經濟犯罪偵查。

一、前言

面對日益氾濫的電信網絡詐騙，我國公安部會同最高法、最高檢、工信部、人民銀行和三大運營商持續開展“斷卡”、“雲劍”、“長城”等專項行動，對電信網絡詐騙犯罪始終保持依法嚴打嚴懲的高壓態勢，極大地震懾犯罪，電信網絡詐騙立案數已從 2021 年至 2023 年連續同比下降。同時，隨着中國、緬甸和泰國聯合打擊跨國電信網絡詐騙犯罪，盤踞在緬北地區的明家、白家和劉家等各類詐騙集團被一舉搗毀，一大批重大犯罪嫌疑人被押解回國，境外詐騙團夥的生存空間受到有力擠壓，電信網絡詐騙犯罪上升勢頭得到遏制。緬北電詐園區的瓦解並不意味着世間不再有“電詐”，電信網絡詐騙依舊會存在，而且會不斷演化新的詐騙手段繼續施詐，電信網絡詐騙犯罪的打擊防範工作是持久戰。

二、電信網絡詐騙的演化分析

目前，眾多電信網絡詐騙團夥都窩藏在境外，國際合作又受到不同國家社會制度和不同法域等因素制約，使得打擊跨國有組織犯罪難以有效及時實施。在嚴厲打擊電信網絡詐騙犯罪的同時，做好廣大群眾的防範工作，提高防詐意識愈發重要。為此，全面分析電信網絡詐騙的演化過程，揭示其本質則是做好群眾防控措施的基本前提。

（一）電信網絡詐騙犯罪本質

《中華人民共和國刑法》第 266 條規定：詐騙罪是指以非法佔有為目的，用虛構事實或者隱瞞真相的方法，騙取數額較大的公私財物的行為。電信網絡詐騙犯罪目前並沒有獨立的罪名，在司法實踐中被廣泛運用，其具體的定義主要是突出了犯罪的技術手段和犯罪行為特徵，即《反電信網絡詐騙法》第 2 條規定：以非法佔有為目的，利用電信網絡技術手段，通過遠端、非接觸等方式，詐騙公私財務的行為。所以說，電信網絡詐騙犯罪本質依舊是詐騙。無論是傳統詐騙還是電信網絡詐騙，詐騙的實質沒變，都是通過傳遞虛假信息，獲取受害人的信任，使用欺詐方法騙取數額較大的公私財物，變化的是犯罪行為特點。

（二）傳統詐騙犯罪與電信網絡詐騙犯罪的關聯

1. 犯罪行為實施由線下特定空域轉化為線上虛擬空間

傳統詐騙犯罪一般是線下實施犯罪行為，多表現為街頭詐騙，即發生在街面或商業場所等人員流動空間。所以，傳統詐騙是多對一的詐騙行為，即多個犯罪分子形成團夥，分工明確，直接面對受害者進行點對點的欺騙活動。線下實施詐騙犯罪自然決定了詐騙犯罪呈現流竄作案，犯罪行蹤不定的特點。而電信網絡詐騙犯罪利用電信網絡技術突破了時間、空間限制，在網絡空間實施非接觸性詐騙活動。一方面，非接觸性詐騙無需面對受害者被騙的慘況，不用體會被騙的痛苦，大大削弱了犯罪分子的犯罪畏懼心態；另一方面，為逃避打擊，大批詐騙集團將窩點轉移至境外，形成境內一些上游環節團夥相互勾連的犯罪鏈組織形式。

2. 詐騙犯罪侵害的對象更加精準

傳統詐騙犯罪主要發生在街頭和商業場所，受害人的出現存在一定的偶然性。詐騙分子也需要根據騙術要求對受害人進行初步的篩選，其過程是詐騙分子依據接觸獲取的周邊信息，依靠個人多年詐騙的識人經驗，並造成與受害人“偶遇”場景。電信網絡詐騙犯罪則是精心選擇詐騙對象。一是通過“信號篩選”模式精準鎖定受害人，即詐騙分子利用詐騙“劇本”，採取大面積群發信息，從海量中選擇回應者。因為信息接受者沒有回應，基本上屬於被識破的情形，騙局結束。若有回應，說明回應者屬於可以進一步誘騙，就會產生第二次信息發送，直至回應者逐漸引入騙局成為受害者。[1] 二是通過非法手段獲取的個人信息，從中精挑細選出滿足詐騙要求的合適對象，進行針對性的騙局腳本設計和話術溝通。例如，“殺豬盤”詐騙根據女性受害者的實際情況和性格，通過精心設計的“劇本”和沉浸式的溝通，誘導女性受害者從好奇和心動逐步發展成網戀關係或是建立起信任關係，一步步陷入騙局。[2]

[1] 牛驚雷、付立柱：〈基於信任生成機理的電信網絡詐騙防控措施研究〉，《河南警察學院學報》，2023 年，第 6 期，第 37–45 頁。

[2] 牛驚雷、付立柱：〈女性受害者視角下“殺豬盤”詐騙中信任關係的形成分析〉，《中國人民警察大學學報》，2023 年，第 2 期，第 5–10 頁。

3. 犯罪行為內容發生迭代

詐騙犯罪主要是通過虛構的事實或隱瞞真相的欺騙方法，誤導或誘騙受害人生成信任，產生錯誤決策，“自願地”將財物交給行騙人或行騙人指定的第三人的行為。傳統詐騙主要實施的犯罪活動包括有利用假冒貴重物品兜售行騙、利用非法外匯交易行騙、利用在國際上不能流通的貨幣行騙、利用“拾金平分”行騙等。[3] 在詐騙過程中主要利用受害人的好心、恐懼和貪心，借助假幣、假寶物等道具和行騙者高超障眼技法，編造虛假事實或隱瞞真相，加上其他團夥人員的配合烘托，誘導受害人被騙。例如，易開罐中獎詐騙是由一夥詐騙分子通過做過手腳的易開罐拉環，在某特定場所製造“中大獎”的事實，團夥在旁邊做托相互配合欺騙受害者花錢買下“中獎拉環”。

犯罪行為存在繼承性。電信網絡詐騙犯罪不斷地升級犯罪手法。目前電信網絡詐騙主要根據詐騙對象情況和性格，分別採取“殺豬盤”詐騙、虛假投資理財詐騙、貸款詐騙、刷單詐騙、註銷“校園貸”詐騙、網絡遊戲虛假交易、冒充“公檢法”詐騙、冒充電商物流客服詐騙等詐騙手法。詐騙內容則緊跟社會熱點問題，時刻保持“與時俱進”變化更新。實施詐騙的工具升級為群發軟體，虛假理財軟體、銀行卡、帳戶和 GOIP 等設備，運用了更為先進的技術，包括區塊鏈、虛擬貨幣、AI 智慧等新技術，實現秒撥、VPN、雲語音、改號呼叫，數位貨幣轉移違法資金，螢幕共用的遠端操控。[4] 例如在“虛假網絡投資理財類詐騙案件”中，詐騙分子通過各種引流方式將受害人拉進各種所謂的投資理財群，群裡其實只有受害人是真正的投資人，其他人包括所謂的理財老師都是詐騙團夥。這種形式的詐騙涉及金融投資方面專業知識，欺騙性更強，不僅損害消費者權益，而且在一定程度上擾亂金融市場秩序。這也意味着電信網絡詐騙犯罪也逐漸向金融詐騙犯罪轉化。

4. 詐騙犯罪組織模式發生變革

傳統詐騙犯罪是組織結構緊湊的結夥犯罪，內部有着結構緊密的組織分工，犯罪行為鏈始終完整，即由犯罪團夥從頭到尾實施完整的詐騙過程，包括詐騙團夥人員招募、詐騙道具購買製作、詐騙內容設計、詐騙過程安排和實施、詐騙錢財分贓和轉移。電信網絡詐騙犯罪則是發生了犯罪組織變革。詐騙團夥內部實現專業分工，組織結構採用金字塔式架構，具體包括“金主”、代理商、管理團隊、人力資源、後勤保障、技術、業務、財務、保安等部門，呈現出多行業支撐、產業化分佈、集團化運作、精細化分工、跨境式佈局等跨國有組織犯罪特徵，[5] 但詐騙犯罪鏈條逐步分化為三個環節，由不同犯罪團夥承擔，進而提升專業化水平。上游有大量卡商、號商將非法獲取的大量銀行帳戶、電話卡、身份證以及 U 盾售賣給中游的洗錢團夥或者直接銷售給下游詐騙團夥，而大量的料商包括一些行業的內鬼將盜取公民的個人信息轉售給下游詐騙犯罪團夥；中游有設備商、引流團夥、包網服務商、網絡商、洗錢團夥為詐騙集團提供技術服務和非法資金轉移服務的犯罪團夥；下游則是組織實施具體詐騙的詐騙犯罪團夥。上中下三個專業犯罪團夥構成了整個詐騙犯罪鏈條，並在各個環節形成各自專業的黑灰產業鏈。犯罪環節的分段不僅提高了犯罪的專業水平和犯罪鏈條複雜化，而且每個環節上的犯罪分子只參與詐騙犯罪行為的一部分，導致其悖德感明顯降低，會認為“我就是爬取一下資料而已 ”，“我只是把銀行卡租借出去 ”。[6] 同時，這也造成涉及的罪名有詐騙罪、幫信罪，以及掩飾、隱瞞犯罪所得、犯罪所得收益罪等，從而加大了偵查的難度。

三、電信網絡詐騙犯罪行為的底層邏輯分析

電信網絡詐騙犯罪的手法和套路是在不斷升級更新，但犯罪行為的底層邏輯並未改變。無論是傳統

[3] 賈克青：〈街頭詐騙犯罪剖析〉，《北京人民警察學院學報》，1999 年，第 2 期，第 4–10 頁。

[4] 新浪新聞，〈公安部：電信網絡詐騙已超 50 種，詐騙手法反覆運算加速！〉，發佈日期：2022 年 4 月 14 日，網址：https://news.sina.cn/gn/2022-04-14/detail-imcwipii4246003.d.html，到訪日期：2024 年 2 月 10 日。

[5] 人民網，〈公安部：電信網絡詐騙犯罪已成為全球性打擊治理難題〉，發佈日期：2022 年 7 月 25 日，網址：http://society.people.com.cn/n1/2022/0725/c1008-32484865.html，到訪日期：2024 年 2 月 10 日。

[6] 李佳鵬、孫韶華、張莫等：〈花樣翻新，類型不下 50 種，防範電信網絡詐騙仍需加力〉，《經濟參考報》，2022 年 3 月 28 日。

詐騙，還是電信網絡詐騙都是通過一定的技術手段，抓住被害人的心理或是人性弱點，利用信息不對稱的優勢騙取被害人信任，誘騙被害人陷入騙局，錢財被騙。因此，信息不對稱就是詐騙犯罪得以成功的底層邏輯。

（一）電信網絡詐騙犯罪的信息不對稱現象

信息不對稱理論闡述了在市場交易中，掌握信息充分的一方擁有比較優勢，出於謀取自身更大的利益，造成信息貧乏的一方處於劣勢，利益會受到損害。從定義上看，由於交易主體掌握信息的差異，反映了信息的分佈及其交易狀況的特性，使得信息不對稱理論成為描述和解釋社會經濟活動的重要工具。[7] 信息不對稱作為電信網絡詐騙犯罪的行為邏輯，形成一個系統過程。[8] 要揭示這一犯罪行為的底層邏輯的運行機理，必須構建電信網絡詐騙犯罪信息傳遞鏈，分析信息不對稱的生成過程。

1. 電信網絡詐騙犯罪信息傳遞鏈分析

在非接觸式的電信網絡詐騙犯罪中，騙取被害人信任是非常重要的環節。在網絡虛擬世界裡，信息傳遞是信任構建的主要媒介。根據 Spence 的信號理論，詐騙犯罪中詐騙分子與受害者之間信任的形成是一種信息傳遞過程。從信息傳遞的全鏈條過程切入分析，我們構建的電信網絡詐騙犯罪過程中信息傳遞鏈如下（圖 1 所示）[9]：

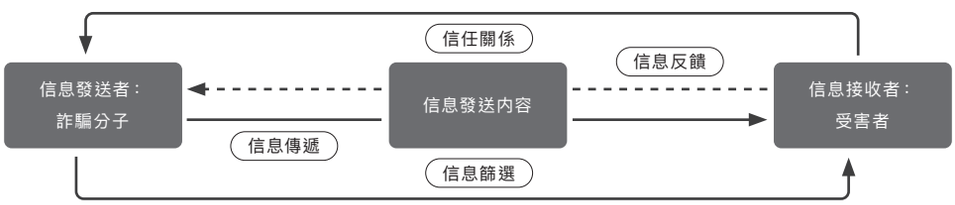

圖1　電信網絡詐騙犯罪信息傳遞鏈

電信網絡詐騙犯罪的整個信息傳遞鏈主要包括三個要素，即信息發送者（詐騙分子）、信息、信息接收者（受害者），構成“信息發送者（詐騙分子）——信息（詐騙劇本）——信息接收者（受害者）——信息反饋（信任）”的信息傳遞鏈邏輯。[10] 無疑，信息不對稱就是在由詐騙分子發佈詐騙信息，通過電信網絡傳遞信息和受害者接收信息構成的鏈條中生成並運行。

2. 電信網絡詐騙犯罪信息不對稱產生過程分析

信息不對稱主要產生於兩個環節。一是受害人個人信息暴露形成受害人與詐騙分子之間的信息不對稱。作為有預謀的詐騙分子，在實施詐騙之前會做好“功課”，與料商進行黑市資料交易獲取大量的公民個人信息，通過傳遞預先設計的信息，測試、觀察和套取信息接收者的性格特徵，以便篩選出具有容易產生信任性格特徵的信息接受者作為繼續推進詐騙的對象，[11] 在全面剖析受害者的基礎上，針對不同職業、性格，甚至不同實際需求編造詐騙內容，合理塑造人設，以確保詐騙過程中自己的特長得到最大程度發揮，做到“知己知彼”。這一精心的篩選過程就決定了在詐騙犯罪整個過程中從一開始，受害者就處於信息缺乏的劣勢方。二是詐騙分子在掌握受害者基本情況和相關性格特徵後，作為信息的優勢方，利用專門設置的詐騙內容，完全操控整個詐騙進程。在傳遞詐騙信息的過程中，根據進程設置相應語義情境和虛假內容，加以各種虛假圖片，微小返利等工具配合，利用近似完美的話術引導受害者對其指令生成依賴、緊張、盲從等情況，從而促使受害者陷入錯誤的認知陷阱，做出錯誤決策。

---

[7]　韓志明：〈跨越信息不對稱的陷阱：國家治理現代化的信息維度〉，《江蘇社會科學》，2024 年，第 1 期，第 86–96 頁。

[8]　饒贊：〈論詐騙犯罪過程中的信息不對稱〉，《湘潭大學 2010 年碩士學位論文》，第 10 頁。

[9]　同註 1。

[10]　李輝、王娜：〈警民信任源於何：基於信號傳遞鏈邏輯的解釋〉，《中國人民公安大學學報（社會科學版）》，2020 年，第 6 期，第 82–98 頁。

[11]　同註 1。

反觀受害者由於自身因素，對一些詐騙內容所涉及的情況不了解，例如：不了解網上購物退款客服流程、公安辦理各類案件規定、銀行借貸具體要求等社會行業基本工作標準流程，從而對電信網絡當中的“公安民警”、“檢察官”、“購物平台客服”、“貸款公司高管”等虛構人物的深信不疑。在信息掌握完全不對等的情況下，受害者陷入詐騙是自然的。

（二）電信網絡詐騙犯罪信息不對稱產生根源分析

1. 公民個人信息洩露和侵犯個人信息是信息不對稱生成的首要原因

公民個人信息的洩露和侵犯一般集中在通信、銀行、保險、房產、酒店、物業、物流等行業領域。這些行業領域管理不善，存在着大量的“內鬼”為了個人利益，售賣公民個人信息。2021 年全國公安機關抓獲行業內部人員 680 餘名，全國檢察機關起訴侵犯公民個人信息的行業“內鬼”500 餘名。[12]2021 年侵犯公民個人信息十大典型案例顯示侵犯公民個人信息的手段主要有利用外掛程式、木馬釣魚病毒等技術竊取使用者手機信息、上網標籤、註冊遊戲帳號、快遞信息販賣給詐騙團夥。[13]

2. 傳遞的詐騙內容是信息不對稱生成的關鍵原因

詐騙內容之所以能夠矇騙受害人主要原因，在於詐騙內容是詐騙分子精心打造的有針對性的話術和劇本。有些內容是根據國家社會經濟戰略發展規劃精心創作，緊貼社會生活的熱點問題，例如，“萬眾創業”、“地攤經濟”、“碳中和”、“養老經濟”和“數字貨幣”等，從而具有較強的迷惑性；有些內容具有行業特點，對於受害者來說相對陌生，甚至神秘。例如，不清楚網絡購物退款流程，受害者在無意識狀態下將個人帳戶驗證碼提供給虛假的“平台客服”；在“冒充公檢法詐騙”中，受害者不了解政法部門日常對外業務，加上出於對公共權威的敬畏，對冒充公檢法幹部的詐騙分子所下達的指令深信不疑，毫不懷疑地按照要求，將自己“涉案”帳戶裡的資金轉入所謂的“安全帳戶”進行安全審查和隔離保護。[14] 而且詐騙內容都是來源於生活，有其真實的一面。這也是受害者深信不疑的原因，但關鍵的是這些內容對於受害者來說，由於不熟悉而缺乏正確認識，處於特定場景中，信息不對稱的劣勢促使受害者在短時間內極易做出錯誤決定。

3. 傳遞技術為信息不對稱的生成提供了保障

一是詐騙分子塑造各種符合詐騙內容的虛假身份。有滿足面孔可信度 [15] 的“白富美”、“高富帥”；有容易產生信任的具有較高社會地位、能力特質突出“成功人士”、有身穿制服，手持證件的“公檢法人員”。為了進一步佐證詐騙分子虛構身份的真實，詐騙分子還加以各種伎倆提升行為可信度，[16] 推進受害者生成錯誤認知。例如，利用受害者嘗試性地小投資，獲得較高回報來驗證詐騙分子所具有的特質能力：有不一般的社會關係、在大數據處理方面的超人技能，或掌握某些博彩網站的漏洞，從而增加受害者對詐騙分子身份的信任。

二是營造特殊語境擴大受害者性格弱點，加大受害者信息不對稱的劣勢。一方面，在信息傳遞過程中，詐騙分子通常是以敘事性方式講授個人經歷，以拉近與受害者之間的距離，產生共鳴且形成情感建構的效應，[17] 從而加強對詐騙分子的信任。另一方面，製造緊急情境加劇受害者緊張情緒。詐騙分子會安排製造一系列緊急情況，例如告知受害者“帳戶涉嫌洗錢”、“行為違規影響個人誠信”，同時配置虛假網絡頁面、假通緝令等圖片，再通

[12] 靳高風、張雍錠、郭兆軒：〈2021—2022 年中國犯罪形勢分析與預測〉，《中國人民公安大學學報（社會科學版）》，2022 年，第 2 期，第 1–12 頁。

[13] 中華人民共和國最高檢察院，〈檢察機關全鏈條懲治電信網絡詐騙犯罪 2021 年起訴 4 萬人〉，發佈日期：2022 年 3 月 2 日，網址：https://www.spp.gov.cn/spp/xwfbh/wsfbh/202203/t20220302_546333.shtml，到訪日期：2023 年 2 月 27 日。

[14] 同註 1。

[15] 可信度（trustworthiness）指被信任方可以被信任或者依賴的程度。可信度作為被信任方自身特質直接影響雙方信任關係的建立。可信度分為面孔可信度和行為可信度兩種類型。

[16] 行為可信度指由被信任方的行為特徵所決定的其自身可以被信賴的程度，如通過信任雙方的直接交往或是通過其他渠道得知的有關個體日常行為中表現出的善良、正直等相關的行為信息。引用 Zucker, L. G. Production of trust: Institutional sources of economic structure, 1840–1920[J]. Research in Organizational Behavior, 1986，8(2):53–111. 參見梅晶：〈面孔可信度對信任行為的預測：一般信任傾向的調節作用〉，《浙江師範大學碩士學位論文》，2017 年，第 6 頁。

[17] 葉洪、段敏：〈“殺豬盤”網絡詐騙行為的個案分析與模擬實驗研究〉，《中國人民公安大學學報（社會科學版）》，2020 年，第 5 期，第 10–16 頁。

過以急迫的“查案和詢問”加快各環節緊扣的時間和營造緊張氣氛，甚至命令受害者自我設置封閉空間，切斷與外部聯繫，使其陷入緊張無助的困境，喪失心理抵抗力，無形之中放大了受害者劣勢狀態，壓迫其從潛意識裡產生“避免損失”的本能，在慌忙之中陷入偏執性判斷，完全聽從詐騙分子指令。[18]

四、電信網絡詐騙犯罪防控體系建設

雖然 2021 年全國檢察機關起訴電信網絡詐騙犯罪 4 萬人，同比下降了 20%，[19] 但電信網絡詐騙犯罪不會削弱，還會利用各種新技術、新的應用場景等因素進行犯罪行為裂變，演化出新的犯罪業態。目前，依舊嚴峻的電信網絡詐騙犯罪形勢也說明了電信網絡詐騙犯罪不是簡單的社會治安問題，而是複雜的社會治理難題，[20] 其打擊防控工作是長期性的。打擊是威懾的重要手段，在犯罪問題的治理上存在被動性。建立有效的防控體系，對於全面提高電信網絡詐騙犯罪的治理水平會起到事半功倍的效果。

（一）加強個人信息安全保護，切斷信息不對稱源頭

通過前文分析，電信網絡詐騙犯罪之所以容易成功，與詐騙分子提前精準掌握詐騙對象的大量個人信息有密切關係。公民個人信息的洩露和盜取使得受害人在詐騙過程中完全處於被操縱狀態，實施精準詐騙，而且高額非法收益又衍生出侵犯公民個人信息罪行為。2021 年全國公安機關破獲侵犯公民個人信息案件 9,800 餘起，抓獲犯罪嫌疑人 1.7 萬餘名。[21]2021 年全國檢察機關起訴侵犯公民個人信息犯罪嫌疑人 9,800 餘人，同比上升 64%。[22]2021 年全國人民法院審結利用各種形式竊取、釣魚欺詐、販賣個人信息犯罪相關案件 4,098 件，同比上升 60.2%。[23]

目前侵犯公民個人信息犯罪行為主要包括信息盜取、提供和倒賣三大環節，公安機關針對相應環節分別構建了針對性的偵查打擊策略。通過發起打擊駭客犯罪集群戰役，偵破一批利用木馬病毒、釣魚網站、滲透工具、網絡爬蟲等駭客手段竊取公民個人信息案件，全面清理侵犯公民個人信息犯罪的技術交易源頭；針對行業內部洩露問題，協同電信運營商、醫院、保險公司、房地產、物業、快遞等行業，開展個人信息洩露治理專項行動，打擊行業“內鬼”，加強行業職操監管；通過買賣信息線索鎖定那些從事公民個人信息的銷售網絡平台，壓縮資料中間商和物料供應商的生存空間。[24]

在打擊侵犯公民個人信息罪的同時，必須系統全面加強個人信息保護。2021 年 6 月，全國人大常委會審議通過了《數據安全法》，8 月通過了《個人信息保護法》，不僅在立法上對個人信息安全作出了法律保障，也為全面提高社會安全行業管理和源頭治理，有效打擊侵犯公民個人信息罪提供了法律支援。公安機關在綜合治理的過程中，以問題為導向，在互聯網平台日常執法監督檢查中，聯合網信、工信等部門，加強網絡資料的安全防護和安全責任落實，同時向群眾開展宣傳教育，普及個人信息保護知識和注意事項，切實形成保護公民個人信息和數據安全的工作合力。[25]

（二）科學預測詐騙手段變化趨勢，消除信息不對稱運行基礎

1. 根據大數據採擷技術，掌握詐騙內容變化規律，精準預測未來詐騙關鍵詞

詐騙內容是電信網絡詐騙信息傳遞的對象。公安機關提前將其破解，先一步掌握詐騙“劇本”，第一時間發佈權威提示，無疑有助於群眾做好防範措施。[26] 為此，公安機關要運用大數據採擷技術，根據詐騙內容變

[18] 謝玲：〈論跨境電信網絡詐騙案件的打擊困境及破解對策：以“人員流”證據的收集、運用為視角〉，《中國刑警學院學報》，2021 年，第 1 期，第 75–81 頁。

[19] 同註 1。

[20] 浙江新聞，〈持續遏制電信網絡犯罪高發多發態勢〉，發佈日期：2021 年 9 月 17 日，網址：https://zjnews.zjol.com.cn/zjnews/202109/t20210917_23103156.shtml，到訪日期：2023 年 2 月 2 日。

[21] 中華人民共和國中央人民政府，〈“淨網行動”這一年：偵辦侵犯公民個人信息等網絡犯罪案件 6.2 萬起〉，發佈日期：2022 年 1 月 5 日，網址：https://www.gov.cn/xinwen/2022–01/05/content_5666617.htm，到訪日期：2022 年 2 月 5 日。

[22] 同註 17。

[23] 中華人民共和國司法部，《最高人民法院工作報告》，網址：https://www.moj.gov.cn/pub/sfbgw/zwgkztzl/2022zt/2022qglh0222/2022qglhbgyqd/2022qglhfybg/202203/t20220315_450733.html，到訪日期：2022 年 3 月 16 日。

[24] 董凡超：〈築牢維護公民個人信息安全銅牆鐵壁〉，《法治日報》，2023 年 11 月 2 日。

[25] 劉丹、廖澤婧：〈重拳出擊，保護公民個人信息安全〉，《人民公安報》，2023 年 8 月 11 日。

[26] 陸愛紅：〈治理電信詐騙須打擊與防範並重〉，《人民公安報》，2016 年 4 月 14 日。

化規律，通過構建關聯模型不斷學習詐騙內容的敏感欄位，結合社會環境特徵和經濟發展趨勢，實現詐騙新“劇本”精準預測，提高全民防範的針對性。詐騙內容基本都來源社會生活，緊貼熱點問題，不斷變化詐騙手法，更新犯罪技術，使犯罪更加隱蔽，也更具迷惑性。[27] 諸如，“網絡購物詐騙”、“網絡遊戲詐騙”、“冒充好友詐騙”等詐騙與人們日常社會中網絡應用極高有關。“移動社交、移動視頻、移動購物的活躍滲透率均在90% 以上”；[28]“投資理財詐騙”、“帳戶涉嫌洗錢或涉稅詐騙”等詐騙所涉及的投資、理財、稅收，甚至洗錢都是我國市場經濟不斷深化發展過程中的產物和現象；“養老投資詐騙”、“養生保健詐騙”等詐騙也是詐騙分子利用我國正在探索養老產業市場化發展的相關政策。所以，運用大數據構建模型，學習詐騙劇本語義環境和與關鍵字的相關規律，根據我國未來社會、經濟以及科技發展新態勢，加快計算未來詐騙關於諸如“金融創新”、“區塊鏈”、“虛擬貨幣”、“元宇宙”、“AI 智慧”等情境內容，實現精準反詐防範和宣傳。

2. 掌握詐騙犯罪手段變化動態，明確公安打擊方向

當前電信網絡詐騙犯罪組織多以現金網公司、博彩公司、科技公司等形式，採取產業化和企業化對外運行模式，內部組織嚴密、分工明確、管理高效，專業化程度極高，[29] 不僅具有極強的迷惑性，也加大了公安偵查打擊難度。究其根源在於犯罪組織的產業化和專業化。犯罪組織的產業化和專業化有助於詐騙犯罪手段產生新變化——複合化，以加大迷惑性和反偵查效果。詐騙通過網絡技術實現了詐騙涉眾面廣，要提高詐騙的迷惑性，不僅要推進犯罪手段複合化，更要結合專業化。2021 年 8 月以來，以“兼職刷單”、“戀愛交友”為開端，融合“殺豬盤”、虛假貸款等多種詐騙手段的複合型詐騙案件高發，已成為當前電信網絡詐騙犯罪中變種最多、變化最快的一類。[30] 金融創新業務明顯符合專業化的要求，電信網絡詐騙犯罪與金融詐騙犯罪交織一起，詐騙手段更加專業，無疑會進一步增加偵查打擊難度。除此之外，還有利用曝光受害者隱私的“裸聊詐騙 + 敲詐”、“交友聊天 + 賭詐”結合等新的犯罪手段。為此，做好相關部門信息共用，強化技戰法相互學習，是提高部門協同打擊效能的必要前提。

（三）構建精準的群眾預防宣教體系，改變信息不對稱中劣勢地位

針對詐騙分子的精準詐騙，我們的宣傳也應構建精準的反詐宣傳體系。

1. 根據受害者性格特徵分析，優化反詐宣傳邏輯思路

在電信網絡詐騙中，受害者具有容易生成信任的性格特徵也是被詐騙的關鍵原因之一。這也是詐騙分子前期進行詐騙對象篩選的目的。目前我們不斷加大了反詐宣傳力度，但各種詐騙案件依舊發生，一些受害者依舊陷入老套的騙局，甚至面對勸阻的民警產生極大的不信任。其中問題在於我們的反詐宣傳更多的是一種面對大眾的普遍宣傳，是一種大水漫灌式宣傳。其結果是沒有針對性，感覺別人的教訓與己無關，宣傳沒有深入人心。要實現精準反詐，必須優化反詐宣傳邏輯思路。一是運用大數據技術分析，從大量詐騙案例中梳理不同類型詐騙所塑造人設和情景，總結出在詐騙過程中容易產生信任的受害人性格特徵，由此確立潛在受害者的人群範圍，再根據詐騙類型有針對性地開展反詐教育宣傳。二是根據電信網絡詐騙犯罪案件中受害人出現老年人和未成年人被害率較高趨勢，加大反詐宣傳和社會幫扶的協同治理。未成年人多以直播打賞、網絡遊戲、網絡購物等形式被騙，而老年人則多因養老投資、養生保健、情感交流等幌子落入圈套。[31] 關注未成年人和老年人的身心健康是需要各級政府部門、學校、社區和家庭共同攜手給予關愛服務、心理疏導和家庭教育指導。

2. 公開透明相關行政部門和行業的業務流程，提高群眾的信息優勢

在詐騙中，由於對相關政府和行業業務流程的不了解，成為詐騙分子矇騙群眾的關鍵，也是受害者

[27] 同註 5。

[28] 同註 6。

[29] 王曉偉、趙照：〈電信網絡詐騙犯罪人員流的構成與偵查方法研究〉，《中國人民公安大學學報（社會科學版）》，2022 年，第 4 期，第 53–64 頁。

[30] 同註 6。

[31] 同註 12。

在信息不對稱中劣勢產生的原因之一。要提高群眾的信息優勢，必須説明群眾全面了解政府部門和行業對外的業務流程。所以，反詐宣傳應增加涉及群眾切身利益的業務辦理流程的講解。例如，公檢法機關通過公開基本業務流程，消除群眾對公檢法業務的“神秘感”；金融機構通過宣講國家金融政策，各種理財產品特點和存在的可能風險點，提高群眾金融風險意識；知名購物平台要利用多種渠道説明網絡購物各項服務流程，消除服務環節中的“盲點”，通過提高群眾對各種信息的掌握程度，改變群眾在詐騙中信息不對稱的劣勢地位。

（四）以制度創新增強警民之間的制度信任，築牢反詐治理的社會基礎

制度信任是在法律規範的基礎上生成的，遵循制度約束的理性信任。由於制度能夠在社會運行中通過建立秩序，降低社會的高度複雜性和高度不確定性，增強個體行為人的理性選擇，[32] 甚至在一定程度上調節了日益充滿張力的人際信任。[33] 制度信任在現代社會良性運行和協調發展中的重要性越發凸顯，[34] 同理警民之間的制度信任直接關係基層警察與社區居民的警群關係，影響着公安機關基層社會治理水平和效能。

1. 創新多元基層社會治理模式，改進警民制度信任

基層社會治理（包括治安治理）是多元主體參與治理的活動。依靠群眾、發動群眾和凝聚群眾是公安工作的群眾路線具體內容。僅依靠社會監督和群眾投訴等制度難以建立親密警民關係，反而可能滋生抱怨的負面情緒，自然影響群眾參與社會治理的積極性，從而造成單純以制度信任為基礎所形塑的警民信任關係不斷弱化。[35] 創新基層社會治理模式必須提高制度建設的科學性。科學性體現在制度經歷實踐檢驗，並在實踐中通過評估和回饋機制得到不斷完善。為此，社會治理要在制度上賦予社會組織、群眾在制度執行過程中科學評價制度有效性的機會，[36] 促進警民之間形成民警真實充分了解群眾訴求，不斷提升執法水準，群眾不再做“旁觀者”，積極參與治理和績效評估，逐步建立起共建共治共用理念的制度信任。

2. 以問題為導向，解決群眾切身利益，營造提升制度信任的社會環境

要提升警民制度信任水平，社會治理制度必須確保對群眾利益的維護和保障。只有人民獲得更多、更直接、更實在的獲得感、幸福感、安全感，才能保持制度優勢的可持續發展。公安機關在構建反詐防控體系建設中，要通過開展接待日、走訪調研等活動積極公開工作業務流程和政務信息，將公安民警的職責和執法要求向群眾擺明，要以解決群眾最關心、最直接、最現實的利益問題為驅動力，吸引群眾真心加入社會治理行動中，通過營造“公平、公正、公開”的社會環境，提高警民制度信任，實現既能深入了解社會民情，掌握群眾基本訴求，又能接受群眾監督，加強執法公正，築牢反詐治理的社會共治防線。

五、總結

電信網絡詐騙犯罪會長期存在是一個客觀事實。我們必須清楚地認識到打擊防範電信網絡詐騙犯罪是持久戰，同時，也要意識到這是一個複雜的社會治理難題。有效的防範不能單靠公安機關的依法嚴厲打擊，更需要多部門、各行業、眾多社會組織和廣大群眾參與到電信網絡詐騙犯罪防控體系的建設中，通過落實各級政府部門和行業監管主體責任，將管控治理工作納入績效考評，從制度上推進協同共治，通過基層社會治理模式創新，構建全社會參與共治防線，合力擠壓犯罪空間，[37] 守護好群眾的“錢袋子”。

---

[32] 戚玉覺、楊東濤、何玉梅：〈組織中的制度信任：概念、結構維度與測量〉，《經濟管理》，2018 年，第 2 期，第 192–208 頁。

[33] 鄒宇春：〈提升制度信任：確保政府良性運行的重要方向〉，《中國發展觀察》，2014 年，第 8 期，第 28–30 頁。

[34] 周延東、閆煜：〈“制度──關係”互構視閾下的警民信任研究〉，《中國人民公安大學學報（社會科學版）》，2022 年，第 1 期，第 149–156 頁。

[35] 同註 32。

[36] 同註 1。

[37] 中國青年網，〈公安部：打擊電詐犯罪成效顯著成功避免 6178 萬名群眾受騙〉，發佈日期：2022 年 4 月 14 日，網址：https://news.youth.cn/gn/202204/t20220414_13611187.htm，到訪日期：2023 年 2 月 18 日。

電信網絡詐騙關聯犯罪治理研究
——以幫信犯罪為視角

王彬 *

摘要：幫信犯罪是電信網絡詐騙的關聯犯罪，是電信網絡詐騙的重要支撐和基礎。幫信犯罪有特定的內涵、特點與類型。幫信犯罪治理涉及到諸多環節和諸多方面，在治理過程中也面臨着諸多治理困境，這些治理困境主要表現為事前預防之困境、事中阻斷之困境和事後懲治之困境。面對我國幫信犯罪治理過程中存在的諸多困境，應當立足於我國幫信犯罪發生、發展和完成的實際情況，多措並舉，綜合施策，有針對性地加以系統破解。只有這樣，才能有效遏制幫信犯罪高發、多發勢頭，取得真正的治理質效。

關鍵詞：幫信犯罪 主要類型 治理困境 破解對策

Research on the Governance of Telecommunications Network Fraud Related Crimes-From the perspective of crime of aiding information network criminal activities

Wang Bin

Abstract: Crime of aiding information network criminal activities a related crime of telecommunications network fraud, which is an important support and foundation of telecommunications network fraud. The crime of aiding information network criminal activities has specific connotations, characteristics, and types. The governance of crime of aiding information network criminal activities involves many links and aspects, and also faces many governance difficulties in the governance process,these governance difficulties mainly manifest as the dilemma of pre prevention, the dilemma of blocking during the process, and the dilemma of post punishment. In the face of many difficulties in the governance process of crime of aiding information network criminal activities, we should base ourselves on the actual situation of the occurrence, development, and completion of crime of aiding information network criminal activities in our country, take multiple measures, comprehensively implement policies, and systematically crack them in a targeted manner. Only in this way can we effectively curb the high and frequent occurrence of crime of aiding information network criminal activities, and achieve true governance quality and efficiency.

Keywords: Crime of Aiding Information Network Criminal Activities; Main Types; Governance Dilemma; Cracking Measures

* 王彬，河南警察學院法學教授、鄭州大學法學院訴訟法專業碩士研究生導師，法學博士、博士後。

一、前言

近年來，作為電信網絡詐騙的關聯犯罪，幫信犯罪的發案數量快速增長，一度成為我國位居前三的刑事犯罪類型。2023 年，檢察機關“依法起訴電信網絡詐騙犯罪 5.1 萬人、幫助信息網絡犯罪 14.7 萬人、網絡賭博犯罪 1.9 萬人，同比分別上升 66.9%、13% 和 5.3%”。[1] 可見，雖然經過嚴厲打擊治理，幫信犯罪仍在高位運行。幫信犯罪是電信網絡詐騙的重要支撐與基礎，能否有效治理幫信犯罪，摧毀電信網絡詐騙的重要支撐與基礎，對於遏制我國電信網絡詐騙高發、多發勢頭，進而全面有效治理電信網絡詐騙，保障公民的財產安全和其他合法權益，維護社會治安秩序穩定等，都具有十分重要的意義。基於此，有必要對幫信犯罪的概念、特點與主要類型，治理過程中所面臨的各種困境進行全面、深入的研究與分析，探求破解治理困境的相應對策，以服務於我國幫信犯罪的治理實踐。

二、幫信犯罪及其主要類型

（一）幫信犯罪的概念與特點

幫信犯罪是《刑法修正案（九）》增設的一種犯罪，全稱為“幫助信息網絡犯罪活動罪”，是指行為人明知他人利用信息網絡實施犯罪，為其犯罪提供互聯網接入、伺服器託管、網絡存儲、通信傳輸等技術支持，或者提供廣告推廣、支付結算等幫助的犯罪行為，是電信網絡詐騙犯罪的重要“幫兇”。簡言之，就是在明知他人利用信息實施電信網絡詐騙犯罪的情況下，行為人仍然為其提供幫助的行為。

（二）幫信犯罪具有以下特點：

第一，涉罪主體分佈地區廣泛，低齡化特點明顯。近年來，我國公安司法機關依法查處的幫信犯罪之涉罪主體遍佈全國各個省份，特別是電信網絡詐騙高發、多發地區，依法查處的幫信犯罪之涉罪主體相對較多。從幫信犯罪之涉罪主體年齡結構來看，低齡化特點明顯，“30 歲以下的佔 64.8%，18 至 22 歲的佔 23.7%。犯罪行為人中，低學歷、低收入群體佔多數，初中以下學歷佔 66.3%、無固定職業的佔 52.4%，犯罪行為主要表現為非法買賣‘兩卡’”。[2]

第二，幫信行為具有多樣性。從查處的幫信犯罪來看，幫信行為主要有以下幾種：一是非法提供（出租、出賣）銀行卡、手機卡，“三件套”“四件套”，為電信網絡詐騙提供轉移支付、套現、取現的工具；二是“話務引流”，為電信網絡詐騙欺騙、引誘被害人員；三是提供（出租、出售）營業執照、對公帳戶，為電信網絡詐騙“跑分洗錢”；四是出租、出售支付寶帳號、微信帳號，以及為電信網絡詐騙提供技術支持、技術服務、技術設備等，如提供批量註冊軟體、GOIP 設備、秒撥 IP 等。

第三，幫信犯罪的組織化模式較為常見，分工細化特點突出。實踐中，幫信犯罪多採取“卡農—卡商—卡頭”的組織模式與分工，以團夥形式組織實施。在這種組織模式與分工中，犯罪鏈條最底端的是“卡農”，其負責收購持卡人實名辦理的銀行卡、手機卡，當“卡農”收購的銀行卡、手機卡達到一定的數量後，通過快遞或者直接送達的方式送到“卡商”指定的地點；“卡商”下面有多個“卡農”，當其下面的多個“卡農”將銀行卡、手機卡通過快遞或者直接送達的方式送給“卡商”後，“卡商”再把更多的銀行卡、手機卡通過一定的方式送達給“卡頭”。從表面上看，幫信犯罪似乎無組織、無指揮，十分鬆散，但實際上，團夥內部則組織嚴密，分工明確，發現和治理難度很大。

此外，幫信犯罪還具有網絡化、非接觸性和一定的高科技性等特點。

（三）幫信犯罪的主要類型

幫信犯罪是電信網絡詐騙關聯犯罪，既包括“話務引流”，出租、出售“兩卡”或者出租、出售支付寶帳號、微信帳號構成的幫信犯罪，也包括買賣營業執照、對公帳戶、“跑分洗錢”構成的幫信犯罪。

---

[1] 中華人民共和國最高人民檢察院網站：https://www.spp.gov.cn/spp/gzbg/202403/t20240315_649603.shtml，到訪日期：2024 年 3 月 26 日。

[2] 新浪網：https://k.sina.com.cn/article_1689502037_64b3c155019016fuu.html，到訪日期：2024 年 3 月 28 日。

1.“話務引流”類幫信犯罪

在該類幫信犯罪中，犯罪行為人從上到下分為核心成員、“組長”、“質檢員” 、“話務員”(客服)等不同層級，核心成員負責對接境外詐騙團夥，從境外獲取潛在被害人的名單和電話信息，並將名單分包給“組長”，“組長”負責在網絡招聘平台發佈招聘信息，招募兼職“話務員”。上崗前，“組長”會對新“話務員”進行培訓、傳授話術，組織其運用境外虛擬話務軟體給“潛在用戶”撥打電話，引流到指定聊天室。“話務員”上班時只負責撥打電話，使用不同話術，在“遊戲客服”、“機構客服”、“平台客服”等角色中切換。為了保證通話品質及監督“話務員”按時完成工作，“組長”還招募“質檢員”負責每日調取各“話務員”的通話錄音，監督、甄別“話務員”是否按照“組長”所給的話術誘騙被害人。整個引流幫信活動各環節組織嚴密、各司其職、環環相扣。

2. 買賣營業執照、對公帳戶、“跑分洗錢”類幫信犯罪

“絕大多數的電信網絡詐騙都伴隨着一個黑灰產業鏈，用以買賣手機卡、營業執照、對公帳戶、銀行卡，為各種電信網絡詐騙違法犯罪提供便利”。[3]

買賣營業執照、對公帳戶的基本情形為：首先，開設帳戶：有人以中間人或者“法人代表”身份，召集社會閒散人員或者以給錢讓他人幫忙的名義，註冊企業、開設企業對公帳戶。其次，轉手販賣：買家以每套幾百元至幾千元不等的價格收購包含工商營業執照在內的銀行對公帳戶，再以每套 5,000 到 6,000 元的價格，轉手賣給電信網絡詐騙團夥或者犯罪行為人或者直接銷往境外。這些對公帳戶實際上成為電信網絡詐騙團夥或者犯罪行為人用來洗錢的帳戶。

“跑分洗錢”主要是通過“兩卡”完成的，即電信網絡詐騙團夥或者犯罪行為人詐騙得手後，將詐騙所得贓款通過銀行卡進行層層分流，或者取出或者購買貴重物品，或者進行其他交易行為，將詐騙所得贓款化整為零，進行“洗白”。從治理實踐來看，一些人為了謀利或者基於其他原因，將自己的身份證、“兩卡”出租、出售給電信網絡詐騙團夥或者犯罪行為人後，基本上被用於“跑分洗錢”，這樣出租人、出賣人就會構成幫信犯罪，成為幫信犯罪的涉罪主體。“進城務工人員、偏遠地區人員、在校大學生是出售個人信息的主要群體，這些個人信息被賣到‘卡農’手中，再層層加價賣給電信網絡詐騙團夥或者犯罪行為人用於違法犯罪活動”。[4] 此外，一些人在互聯網上搭建第三方平台、第四方平台，幫助電信網絡詐騙團夥或者犯罪行為人轉賬、提現，也是一種“跑分洗錢”行為，也構成幫信犯罪。

3. 出租、出售支付寶帳號、微信帳號，提供技術類幫信犯罪

出租、出售支付寶帳號、微信帳號，以及為電信網絡詐騙提供技術設備、技術支持和技術服務等，也是幫信犯罪的主要類型。

就出租、出售支付寶帳號、微信帳號類幫信犯罪而言，涉罪主體主要是在校大學生或者社會上的一些其他人員。一些在校大學生或者出於對出租、出售支付寶帳號、微信帳號可能構成犯罪的情況不了解，或者出於謀取經濟利益或者其他目的，在互聯網上註冊支付寶帳號、微信帳號後，出租、出售給電信網絡詐騙團夥或者犯罪行為人，成為電信網絡詐騙的“遞刀人”；還有一些在校大學生為幫信犯罪團夥或者犯罪行為人拉“微信群”，幫其發展人員在互聯網上註冊支付寶帳號、微信帳號，然後出租、出售給電信網絡詐騙團夥或者犯罪行為人。當然，社會也一些其他人員，特別是一些青年人，出於謀取經濟利益的目的，也在互聯網上註冊支付寶帳號、微信帳號出租、出借給電信網絡詐騙團夥或者犯罪行為人，成為幫信犯罪的涉罪主體。

就提供技術設備、技術支持和技術服務類幫信犯罪而言，主要有以下情形：一是出於“賺快錢”或者“炫耀能力”之動機，向電信網絡詐騙團夥或者犯罪行為人出租、出售技術設備，如提供 GOIP 設備等，成為電信網絡詐騙的“技術助攻”；二是提供專業技術支持、軟體工具，為電信網絡詐騙團夥或者犯罪行為人解決電信網絡詐

[3] 新浪網：http://hebei.sina.com.cn/news/2020-06-09/detail-iircuyvi7472974.shtml，到訪日期：2024 年 3 月 26 日。

[4] 荊楚網：http://news.cnhubei.com/content/2020-05/23/content_13068863.html，到訪日期：2024 年 3 月 28 日。

騙過程中遇到的技術難題，為其提高犯罪效率、降低犯罪成本；三是開發專門用於犯罪的黑產軟體工具，如秒撥IP等，提供給電信網絡詐騙團夥或者犯罪行為人，使其用於電信網絡詐騙犯罪並逃避公安司法機關及其他治理機關、部門的打擊、治理。

三、我國幫信犯罪的治理困境

幫信犯罪治理是一項社會系統工程，涉及到諸多方面和諸多環節，集中體現在事前預防、事中阻斷和事後懲治三個治理環節。從幫信犯罪治理實踐來看，每一個治理環節中都存在着這樣或者那樣的治理困境。

（一）事前預防之困境

事前預防是針對普通民眾的一般性預防，其目的是告知或者警示廣大普通民眾遠離幫信犯罪、自覺抵制幫信犯罪。在幫信犯罪治理過程中，事前預防之困境主要表現為以下方面：

1. 普通民眾對幫信犯罪不了解

幫信犯罪行為本身具有很強的欺騙性，普通民眾根本無法認識到幫信行為是違法犯罪。在這種情形下，普通民眾在主動或者被動地捲入幫信犯罪後而不自知，反而認為自己是憑“本事”掙錢，並沒有違法犯罪。例如，有些在校大學生出租、出售本人銀行卡、手機卡，或者受其他利益驅動在校園內招攬同學收購銀行卡、手機卡，成為“卡商”等情形。對此，有些在校大學生通常並不認為自己的行為是違法犯罪，反而認為自己是在“做生意”，憑自己的“本事”掙錢，其結果必然是觸犯刑律，最終陷入幫信犯罪的“泥潭”之中。同時，農村的留守老人、城鎮的獨居老人也是“卡農”收購銀行卡、手機卡的主要對象，這些留守老人、獨居老人常常會因為不了解幫信犯罪的基本情況、基本流程等，出於謀利或者其他目的將銀行卡、手機卡出租或者出售給“卡農”，構成幫信犯罪而不自知。

2. 相應預防機制尚未構建或者雖有構建但尚不健全，無法發揮預防機制應有的預防作用

從事前預防的實際需求來看，校園預防機制、家庭預防機制和社會預防機制都是預防幫信犯罪不可或缺的必要機制。

校園預防機制、家庭預防機制對於防範、減少在校大學生、青少年捲入幫信犯罪的作用十分明顯；而社會預防機制的適用對象則是全方位的，在防範、減少普通公民、在校大學生和青少年捲入幫信犯罪方面的作用也十分重要。但現實情況卻是，幫信犯罪之校園預防機制、家庭預防機制幾乎沒有構建，充分發揮其作用更是無從談起。幫信犯罪之社會預防機制雖然建立起來，在某種程度上也發揮了相應的作用，但社會預防機制作用的發揮需要公安機關、網絡、電信、銀行、金融等機構、部門的通力合作。實際上，在我國，各社會預防機制構建主體都是在各自的機構、部門內部構建與運行幫信犯罪之社會預防機制，且“各自為戰”，也沒有實現機構、部門社會預防機制之間在數據信息上的互聯互通與共享，其結果必然給幫信犯罪預防帶來諸多困境。

（二）事中阻斷之困境

事中阻斷是指在幫信犯罪發生過程中，擔負幫信犯罪治理之責的相關機關、部門密切配合，多方聯動，通過常規方法或者現代科技方法，及時監測預警，釐清幫信犯罪的鏈條與源頭，有效阻斷幫信犯罪繼續進行的一種治理措施。在事中阻斷環節，主要存在以下困境：

1. 相互配合不足、無法有效監測預警

幫信犯罪的發生、發展與完成涉及到公安機關、網絡、電信、銀行、金融等機構、部門與諸多環節。要實現幫信犯罪的事中阻斷，需要各機關、部門之間各司其職、各負其責，相互配合，切實落實各自的監測預警之責。但實際情況卻是，各相關治理機關、部門之間缺乏應有的配合與協作，各相關治理機關、部門之間也沒有認真履行自己的監測預警之責，導致事中阻斷無法有效進行和發揮應有的作用。例如，在校大學生在校園內或者周邊銀行營業網點、電信營業網點多次辦理銀行卡、手機卡，或者一人辦理多張銀行卡、手機卡時，相關銀行、電信部門應當及時監測預警，並將相關數據信息及時告知或者傳輸給其他相關治理機關、部門，以便它們

能夠及時阻斷幫信犯罪。但是，由於各種因素的影響與制約，相關銀行、電信部門並未及時有效監測和預警，導致一人多次辦卡或者一人辦理多卡的情況時有出現，造成幫信犯罪事中阻斷之困境。

2. 科技反制不力，無法有效源頭治理

“現代科技發展是一柄‘雙刃劍’，在給人們生產、生活等方面帶來各種便利的同時，也給犯罪行為人實施犯罪提供了機會與場所”。[5] 幫信犯罪的發生、發展和完成離不開現代科技的支撐，否則，幫信犯罪將無法實施完成。在幫信犯罪發生、發展和完成過程中，為了逃避公安機關的打擊和其他治理機關、部門的有效監管，幫信犯罪行為人大都通過網絡進行勾通聯繫，實施銀行卡、手機卡等買賣活動，或者利用黑色產業鏈提供的專業技術設備、軟體工具等實施幫信犯罪，這就要求公安機關及其相關治理機關、部門，如網絡、電信、銀行、金融等充分利用現代科技予以反制，從源頭上進行治理，以有效阻斷幫信犯罪的繼續進行。但是，從幫信犯罪事中阻斷的情況來看，公安機關明顯存在着現代科技實力不足，運用現代科技手段反制不力的情況，其他相關治理機關、部門也存在類似或者相同的情況。這種情況的存在必然導致相關治理機關、部門無法有效運用現代科技手段事中阻斷幫信犯罪的發生、發展與完成，更無法從源頭上予以有效治理。

3. 力量資源整合不足，無法有效協作或者合作

幫信犯罪事中阻斷涉及到不同治理機關、部門和不同的環節，任何一個機關、部門缺失，任何一個環節出現疏漏或者弱化，都會影響幫信犯罪事中阻斷的效果。但從我國幫信犯罪事中阻斷實踐來看，力量資源整合存在明顯不足，造成各種力量資源無法形成合力，更無法在事中阻斷中有效開展協同。主要表現為：(1) 高校的各種力量與資源整合不足，導致校園內出租、出售銀行卡、手機卡等幫信犯罪行為無法有效事中阻斷。(2) 公安機關與網絡、電信、銀行、金融等機構、部門的力量與資源整合不足，沒有實現數據信息的互聯互通與共享，導致無法及時有效地阻斷正在發生的幫信犯罪。

（三）事後懲治之困境

事後懲治是指公安司法機關對構成違法或者犯罪的幫信行為人，以及其他相關涉罪主體，依法給予各種處罰或者懲罰的專門活動。幫信犯罪之事後懲治存在以下困境：

1. 口袋罪化趨勢嚴重，影響精準定罪量刑

主要表現為：一是在涉及多個下游幫助行為時，只要查清上游犯罪，下游的幫助行為定為掩飾罪；無法查清上游犯罪時，下游的幫助行為則籠統地一概定為幫信罪。二是幫信罪的認定存在着非此即彼的構罪模式。在訊問中，只要犯罪行為人回答了解或者知道被出租、出售之銀行卡、手機卡等的用途，辦案人員便完成了對於“明知”的主觀推定，犯罪行為人即構成幫信罪。“由於電信網絡詐騙犯罪的層級性、鏈條性，偵查機關也難以確定究竟哪一級為幫助犯，哪一級為正犯，在實踐認定模糊的情況下，統一蓋然認定為幫信罪，是幫信犯罪實踐中口袋化的集中體現”。[6] 由於幫信罪之口袋化趨勢，導致在實踐中難以對幫信罪予以精準定罪量刑。

2. 浪費治理資源，治理成本與治理效益不平衡

幫信犯罪與電信網絡詐騙犯罪之間存在着鏈條化、分工化等特徵，提供銀行卡、手機卡的“卡農”是最容易被查處的一類人，而“卡商”和“卡頭”是負責向“卡農”收購銀行卡、手機卡的兩類人，這兩類人往往隱藏比較深，不易查處。通常情況下，案發後，偵查機關通過銀行轉賬流水去向就能直接抓獲“卡農”，但在大多數情況下則無法直接抓獲“卡商”和“卡頭”，或者抓獲的“卡商”和“卡頭”比較少。如此以來，在治理過程中，大量的治理力量與資源被用於查處從事幫信犯罪行為的“卡農”、“卡商”和“卡頭”，必然“擠

[5] 王彬：〈養老詐騙犯罪的治理難點分析與破解對策探究〉，《浙江警察學院學報》，2023 年，第 1 期，第 79 頁。

[6] 班藝源：〈少捕慎訴慎押下“兩卡”類幫信罪的司法治理〉，《政法學刊》，2022 年，第 6 期，第 15 頁。

佔”用於查處電信網絡詐騙犯罪的治理力量與資源，導致治理力量與資源的投入不夠精準，甚至浪費治理資源，造成治理成本與治理效益的不平衡。

四、我國幫信犯罪治理困境的破解對策

幫信犯罪治理“是一項複雜艱巨的工作，需要不同機關、部門與社會各方面的共同參與，甚至涉及到國際執法合作或者協作的開展，必須多措並舉，綜合施策，才能真正取得實際效果”。[7] 針對幫信犯罪治理過程中存在的諸多困境，可以從以下環節或者方面綜合施策加以破解。

（一）事前預防困境之破解對策

針對幫信犯罪事前預防中存在的諸多困境，可以採取以下對策有針對性地加以破解。

1. 多管齊下，加大反幫信犯罪宣傳的力度與廣度，破解普通民眾對幫信犯罪不了解之困境

一是通過各種新聞媒體，採取普通民眾容易接受的形式與途徑，通過典型案例說明幫信犯罪的基本樣態，如何發生、發展和完成及其社會危害性，使普通民眾自覺樹立反幫信犯罪的意識，提高識別、防範和抵制幫信犯罪的能力與水平，遠離幫信犯罪；在捲入幫信犯罪之後能夠認真對待，採取有效方法或者措施及時從幫信犯罪的陷阱中抽身，並積極配合公安機關等治理機關、部門的治理行為。這種宣傳可以是對幫信犯罪有關法律、法規和政策的解讀、宣講，也可以是對幫信犯罪典型案件的剖析、講解與分析。

二是充分發揮公安機關反幫信犯罪宣傳主力軍作用。作為治理幫信犯罪的專門機關，公安機關也承擔着反幫信犯罪宣傳的責任，因此，公安機關的專業警隊、基層公安派出所、社區警務室等要組織力量深入社區、居民小區及其他相關公共場所，如車站、廣場、商場等開展反幫信犯罪宣傳活動，提高普通民眾反幫信犯罪的能力與水平。同時，要聯合高校的相關機構、部門，針對在校大學生涉幫信犯罪的實際情況，走進高校，全面、深入地開展反幫信犯罪宣傳活動，提高在校大學生反幫信犯罪的能力與水平。

三是充分發揮村民委員會、居民委員會等社會基層自治組織，以及網格化管理員等力量，有針對性地對農村留守老人、城鎮獨居老人開展反幫信犯罪宣傳活動，用發生在老年人身邊的案（事）例“對老年人進行‘點對點’的示範教育，揭露幫信犯罪的‘手法’、‘套路’，不斷提高老年人的識騙、防騙意識與能力，最大限度地擠壓犯罪行為人之‘行騙空間’”。[8] 通過“點對點”的有針對性的宣傳活動，使農村留守老人、城鎮獨居老人對幫信犯罪有一個直觀的認識，即出賣自己的“銀行卡”、“手機卡”就是幫信犯罪，進而促使老年人保存好自己的銀行卡、手機卡，不輕易交與他人或者出租、出售給他人。

2. 建立健全相應預防機制，破解無預防機制或者有機制但尚不健全之困境

一是健全社會預防機制，充分發揮已有預防機制在預防幫信犯罪中的作用。目前，我國已經構建相關社會預防機制，但這種機制尚不健全，沒有形成體系。因此，應當不斷健全已有的社會預防機制，充分利用已有的社會預防機制加強對幫信犯罪及其上游犯罪各種數據信息的監測、預警、處置，防範、遏制各種不良數據信息的傳播與擴散。同時，作為一種電信網絡詐騙的關聯犯罪，幫信犯罪既包括前端的精準獲取公民個人信息、“吸粉引流”、技術支持與技術服務，也包括後端的“跑分洗錢”、支付結算等，情形十分複雜。因此，相關治理機關、部門應當在治理過程中不斷完善已有的社會預防機制，通過已有的社會預防機制及時、準確地對各種幫信犯罪行為進行時時監測預警，阻斷幫信犯罪行為與電信網絡詐騙的各種關聯，使幫信犯罪行為無法完成。

二是構建校園預防機制和家庭預防機制，發揮高校、家庭預防幫信犯罪的能動作用。

首先，構建校園預防機制，充分發揮高校預防機制的作用。在構建校園預防機制的基礎上，形成科學的管理方式、方法，在機制運行與管理過程中注入更多的親情溝通與人性關懷，使在校大學生感受到家庭

[7] 王彬：〈養老詐騙犯罪的治理難點分析與破解對策探究〉，《浙江警察學院學報》，2023 年，第 1 期，第 78 頁。

[8] 王彬：〈養老詐騙犯罪的治理難點分析與破解對策探究〉，《浙江警察學院學報》，2023 年，第 1 期，第 77 頁。

般的溫暖，親人般的呵護，在本人或者同學、朋友捲入幫信犯罪活動，或者發現校園內有幫信犯罪活動時，能夠及時向有關部門或者人員彙報，使校園內的幫信犯罪活動能夠得到及時、有效遏制。從實踐來看，心理因素是在校大學生捲入幫信犯罪活動的一個非常重要的原因，如攀比心理、趨利心理、僥倖心理和跟風心理等，都可能導致在校大學生捲入幫信犯罪活動。因此，應當加強在校大學生的心理健康教育和心理引導，使之具有良好的犯罪防範心理，在接觸或者捲入幫信犯罪活動時，能夠具有相應的判斷、識別與自覺抵制能力，遠離幫信犯罪活動。

其次，構建家庭預防機制，充分發揮家庭預防機制的作用。家庭是在校大學生成長的第一課堂，家風及父母、家人的個人品德修養、言行舉止對子女具有強大的示範、影響作用。同時，長期的共同生活使子女與父母、家人之間形成了緊密的情感（親情）關係，甚至是依戀關係。在校大學生雖然遠離家庭、父母、家人，在異地他鄉求學，但家庭、父母、家人對子女心理、思想和行為的影響仍然十分強大，在某些情況下甚至能夠左右或者決定其心理、思想和行為。因此，在預防過程中，應當充分發揮家庭預防機制在反幫信犯罪中的作用。為此，一是要營造和諧的家庭環境，建立良好的家庭關係，強化家庭的教育功能；二是要優化教育方法，促進社會教育、學校教育與家庭教育的同步與協調；三是要將子女的品德培養與智力培養並重，在培養過程中做到二者的有機統一，不斷增強其抵禦違法犯罪及社會不良風氣影響的能力和抗挫能力，使其能夠自覺遠離各種違法犯罪活動。

（二）事中阻斷困境之破解對策

在治理過程中，只有依憑現代科技，不斷強化現代科技手段應用，整合不同治理機關、部門的資源與力量，才能有效破解幫信犯罪治理事中阻斷之困境。

1. 多方聯動，有效監測預警，破解相互配合不足，無法有效監測預警之困境

一是要強化相關行業、機構、部門的業務風險管控工作。網絡企業、電信運營商、銀行、金融、郵政、快遞行業等應當嚴格遵守相關法律、法規、規章或者制度之規定，加強對相關業務及從業人員的管控工作。例如，銀行、電信部門要加強對本部門工作人員的管控，嚴防本部門工作人員利用職務之便，違法、違規為他人辦理銀行卡、手機卡或者為自己辦理銀行卡、手機卡用於出租、出售。此外，在幫信犯罪治理過程中，要針對普通民眾，特別是在校大學生參與幫信犯罪活動的規律、特點進行研究、分析，精準高效地開展監測預警和風險管控工作，有效阻斷幫信犯罪活動的發展與蔓延。

二是要落實“一案雙查”措施，夯實主體責任。對涉及出租、出售銀行卡、手機卡、微信帳號、支付寶帳號的幫信犯罪，或者提供技術設備或者技術服務的幫信犯罪，偵查機關既要嚴查案件本身，依法追究幫信犯罪行為人的法律責任；也要嚴查與幫信犯罪有關的企業、公司，如互聯網企業、三大電信運營商、銀行等，落實主體責任。工信部、網信辦、人民銀行、市場監管總局等要切實加強對信息類黑灰產業數據信息的監測，不斷提高識別、發現、阻斷黑灰產業的精準度和效率。各地區、各部門要對收購銀行卡、手機卡，或者出租、出售銀行卡、手機卡、微信帳號、支付寶帳號，或者為電信網絡詐騙提供、出售技術設備或者提供技術服務等幫信犯罪活動，及時發現並準確預警，堅決予以阻斷並有效遏制其發展、蔓延。

2. 加強科技反制力度，破解科技反制不力，無法有效源頭治理之困境

事中阻斷幫信犯罪，實現源頭治理，必須加強科技反制力度，以科技對科技，實現科技超越。具體來說，可以採取以下做法：一是採用“發信域名認證”、“發送端阻止”等現代技術，精準識別與攔截幫信犯罪的各種數據信息，實現源頭治理。二是及時下載、拷貝或者採錄相關數據信息，如“QQ 號碼、手機號碼等涉案人員信息；相關 APP、網頁、網址等涉案平台信息；推廣引流、網號、卡號等涉案黑灰產業信息；資金卡、支付寶帳號、微信帳號等涉案資金信息等”[9]，運用現代科技手段或者方法找出相關數據信息的內在規

[9] 王楓梧：〈大學生涉“兩卡”犯罪生成機制及治理對策〉，《江蘇警官學院學報》，2022 年，第 6 期，第 68 頁。

律與關聯性，加強科技反制，實現源頭治理。三是在現代科技支撐下，聯合相關業務機構、部門，搭建反制模型，精準高效地監測與識別涉詐銀行卡、手機卡、支付寶帳號、微信帳號等，實現源頭治理。

3. 整合力量資源，協同治理，破解力量資源整合不足之困境

幫信犯罪治理需要“各行業、各部門共同參與，形成高效的聯動協同機制，才能形成高效的聯動協同治理新格局”。[10]

一是整合高校各種力量與資源，有效阻斷校園內銀行卡、手機卡收購或者買賣活動。為此，高校應當加強對校園內的各種兼職招聘信息的監督與管理，發現與幫信犯罪及黑灰產業有關的招聘信息的，應當及時刪除。高校管理部門及管理人員應當各司其職，各負其責，互通有無，相互配合，動態掌控在校大學生思想動態和行為苗頭，一旦發現在校大學生中存在幫信犯罪的苗頭和實行行為，學校層面要及時干預，或者給予校紀校規處理，或者採取其他教育挽救措施，構成違法犯罪的，由學校保衛部門報告當地公安機關依法作出處理。

二是整合公安機關、網絡、電信、銀行、金融等行業、機構、部門的力量與資源，形成合力，齊抓共管，同向發力。公安機關、網絡、電信、銀行、金融等行業、機構、部門既要各司其職、各負其責，依法嚴格履行自己的職責與義務，又要通力合作，互相配合，互通情報信息，實現數據信息共用。只有這樣，才能改變“各自為戰”的治理格局，形成高效協同、聯動治理的新格局，精準、高效地阻斷幫信犯罪的發生、發展與完成。

（三）事後懲治困境之破解對策

幫信犯罪的事後懲治涉及到公安司法機關和其他相關治理機關、部門，涉及到偵查、起訴與審判等不同訴訟環節，還涉及到行刑銜接問題。因此，破解幫信犯罪事後懲治之困境，可以從以下方面入手：

1. 完善現行立法，明確幫信犯罪的相關問題，破解口袋罪化趨勢嚴重，難以精準定罪量刑之困境

一是修改現行刑法，採取修正案的方式對“幫信犯罪”的具體幫助情形予以明確規定或者列舉，凡是屬於立法明確規定或者列舉的情形之一的，認定為幫信罪，依照幫信犯罪定罪量刑；或者由最高人民法院、最高人民檢察院聯合其他部委以“解釋”、“意見”或者“規定”等形式聯合發佈規範性文件，明確規定或者列舉“幫信犯罪”的具體幫助情形，凡屬於規定或者列舉的情形之一的，認定為幫信罪，依照幫信罪定罪量刑。

二是修改現行刑法，採取修正案的方式對幫信犯罪之“明知”的內涵作出合理界定或者解釋；或者由最高人民法院、最高人民檢察院聯合其他部委以“解釋”、“意見”或者“規定”等形式，對“明知”的內涵作出合理界定或者解釋。

三是修改現行刑法，採取修正案的方式對電信網絡詐騙及其關聯犯罪的層級性、鏈條性等作出明確規定或者列舉，明確哪一層級為幫助犯，哪一層級為正犯，以解決實踐中幫信犯罪認定層級模糊的問題。

2. 合理調配治理力量與資源，依法嚴懲幫信犯罪骨幹分子，破解治理成本與治理效益不平衡，治理資源浪費之困境

一是將治理力量與資源主要投入到電信網絡詐騙犯罪的治理之中，對於幫信犯罪，可以在查處電信網絡詐騙犯罪的同時，投入一定的治理力量與資源展開必要的查處。對於幫信犯罪的立案、偵查與結案應當與電信網絡詐騙犯罪的立案、偵查與結案保持基本的一致性，除幫信犯罪行為較為嚴重外，幫信犯罪一般不易過早結案，應當在查清其幫助、支持電信網絡詐騙犯罪的事實，釐清其實施了哪些幫助行為之後，才能結案。這樣，既達到了懲處幫信犯罪之目的，也達到了懲處電信網絡詐騙犯罪之目的。

二是區別對待幫信犯罪行為人，依法嚴懲幫信犯罪的骨幹分子。從查處的情況來看，有些幫信犯罪行為人，特別是一些在校大學生和青少年，大都是受到“卡農”、“卡商”或者“卡頭”的蒙蔽，或者提供高薪

[10] 同註 7。

工作的引誘才捲入幫信犯罪陷阱的，其實施的幫信行為無外乎就是在銀行、電信部門辦理銀行卡、手機卡出租、出售給“卡農”，或者在互聯網上註冊支付寶帳號、微信帳號等出租、出售給電信網絡詐騙團夥或者犯罪行為人，客觀上社會危害性比較小，絕大多數人在主觀上並不具有“明知”的主觀認識，主觀惡性比較小。因此，對於這一類的幫信犯罪行為人應當採取比較輕緩的懲治措施加以處罰，或者視情節經教育後不予處罰。但對於哪些幫信犯罪的骨幹分子，即“卡商”、“卡頭”，或者黑灰產業鏈上的其他幫信犯罪骨幹分子，如利用職務之便大量辦理銀行卡、手機卡出租、出售謀利的銀行工作人員、電信部門的工作人員，或者提供技術設備、技術服務謀利的企業、公司的技術人員或者其他人員，查清事實後必須依法予以嚴懲，實現源頭治理，既治標也治本。

五、結語

從我國《刑法修正案（九）》的規定來看，幫信罪雖然是輕罪，但從其社會危害性與治理實踐來看，幫信犯罪與電信網絡詐騙的關聯十分緊密，是電信網絡詐騙的重要支撐與基礎，其社會危害性不可低估，治理難度也比較大。近年來，隨着我國打擊治理電信網絡詐騙工作的深入推進，幫信犯罪的打擊治理也逐漸為相關打擊治理機關、部門所高度重視，大量的力量與資源被投入到打擊治理幫信犯罪之中，且取得了不俗的打擊治理效果。但是，應當看到的是，從事幫信犯罪的利益誘惑極大，幫信犯罪的“死灰復燃”性極高，往往會在嚴厲打擊治理後的一段時間內有所收斂，但很快就會“捲土重來”。因此，研究、分析幫信犯罪的概念、特點與主要類型，治理困境，明晰治理困境的破解對策，對於幫信犯罪的專項打擊治理與常態化打擊治理的結合與推進，有效遏制電信網絡詐騙高發、多發勢頭，保護普通民眾的財產安全及其他合法權益，維護經濟社會秩序穩定等方面，都具有十分重要的意義。

非良構偵查情報模糊認知思維的邏輯範式 **

何宏斌、徐為霞、曾木蘭 *

摘要：非良構情報源於偵查實踐認識活動及認識能力的有限性，其在犯罪偵查過程中普遍存在，偵查人員需要借助模糊思維對這類情報作出認知判斷。模糊思維的邏輯要素包括一組情報狀態、一組狀態運算元及相關路徑要素，其邏輯進程是在非良構情報空間中搜索能夠連接情報初始狀態和情報目標狀態的路徑，在認知心理學的問題解決思維理論中，將這種思維邏輯概括為手段──目的。模糊認知思維能力依賴於彌合初始狀態和目標狀態的運算元，其彌合範式表現為選擇、良構、模擬三個遞進的思維層域。此項研究有助於偵查人員理解和提升犯罪偵查中的模糊認知能力，破解非良構情報導致的偵查認知困境。

關鍵詞：犯罪偵查　非良構情報　模糊認知　思維邏輯　思維範式

Logic and Paradigm of Fuzzy Cognitive Thinking in ill-structured Investigative Intelligence

He Hongbin; Xu Weixia; Zeng Mulan

Abstract: Ill-constructed intelligence comes from the limitation of cognition activity and cognition ability in investigation practice. It is common in the process of criminal investigation. Investigators need to make cognitive judgment on this kind of intelligence with fuzzy thinking. The logical elements of fuzzy thinking include a set of intelligence states, a set of state operands and related path elements. The logical process of fuzzy thinking is to search the path that can connect the initial state of intelligence and the state of intelligence target in the ill-structured intelligence space. In the theory of problem-solving thinking in cognitive psychology, this kind of thinking logic is summarized as means - ends. Fuzzy cognitive thinking ability depends on the operator to bridge the initial state and the target state, and its bridging paradigm is represented by three progressive thinking layers: selection, construction and simulation. This research is helpful for investigators to understand and improve the fuzzy cognitive ability in criminal investigation, and to solve the cognitive dilemma caused by ill-constructed intelligence.

Keywords: Criminal investigation; Ill-structured intelligence; Fuzzy cognition； Thinking logic; Thinking paradigm

*　何宏斌，中央司法警官學院，講師，偵查學博士。

*　徐為霞，中央司法警官學院，教授，法學碩士。

*　曾木蘭，中央司法警官學院，講師，法學碩士。

**　基金項目：2023–2024 年度河北省社會科學基金專題項目“數字時代公共安全治理中的網格化三級預警防控機制研究”（HB23ZT018）的階段性研究成果。

一、前言

“情報是為了解決特定問題所需要的知識”。[1] 美國學者大衛·喬納森（David H·Jonassen）根據特定問題的結構特徵，把問題分為良構問題（well–structured problem）和非良構問題（ill–structured problem）。[2] 良構問題是指具備限定性已知條件的問題，並在已知條件範圍內運用相關規則和原理即可進行同一性求解；非良構問題則是具有不確定因素和多樣性求解途徑的問題。在此基礎上，根據知識所解決的特定問題不同，美國學者斯皮羅（R · J · Spiro）將知識劃分為良構領域的知識和非良構領域的知識。[3] 良構知識是指按一定的層次結構組織起來的有關某個待決問題的事實、概念、規則和原理；而非良構知識則是將良構知識應用於具體情勢時有關概念、規則及原理具體適用的知識。

偵查情報揭示特定的案件問題，其理想狀態是有關特定案件的良構情報，在實踐中，偵查情報大多是不確定的、甚至是相互矛盾的非良構情報。良構偵查情報通常包括明確的案件初始狀態、已知的目標狀態、限定的案件空間以及邏輯因素等，通過直接的理解與搜尋過程來實現案件問題轉換，便可啟動與活化。例如：偵查情報中心通報的某兇殺案件現場監控視頻，其適用邏輯是以信息加工理論為基礎的 IDEAL 模式，[4] 即識別（Identifying）、界定（Define）、探索（Exploring）、行動（Acting）、回顧（Looking back）。

非良構偵查情報指向的案件情勢界定不清、目標狀態含糊不明、沒有公認的求解方法及評價標準。例如偵查人員勘驗某襲警案件現場，發現四名被害警員的上衣下邊緣均被略微翻起，這一現象可能是無意造成的，也可能是兇手出於尋槍目的而為。非良構偵查情報通常具有兩個顯著特點：[5] (1) 案件事實的複雜性。非良構偵查情報會同時涉及到許多案件事實，而每一種事實都有其自身的複雜性，且這些事實並不是孤立存在的，而是彼此存在某種聯繫。(2) 情勢的不確定性。每個案件情勢所涉及事實數量和種類不同，而且這些事實的作用、地位以及相互關聯模式也不盡相同。對包含案件事實複雜且適用情勢模糊的非良構偵查情報，不能僅憑某種案件事實、概念、規則及原理為基礎，用已知信息或資料進行簡單啟動，而應在手段——目的思維邏輯的能動牽引下，通過多個事實、概念、規則、原理及大量經驗因素的共同作用，遵循選擇、良構、模擬三個循此遞進的心理層級，實現對非良構偵查情報的傾向性認知，其適用邏輯是以建構理論和情勢認知理論為基礎，包括案件空間的建構、偵查方案的生成與選擇、偵查措施的實施與監測等過程。

二、非良構偵查情報的模糊認知

人們賴以生存的環境往往呈現出“VUCA”狀態，即不穩定（Volatile）、不確定（Uncertain）、複雜（Complex）、模糊（Ambiguous）。在“新冠肺炎疫情（COVID–19 outbreak）”爆發之初的很長一段時間，人們在恐慌之餘也飽受着對病毒來源的各種心理折磨，時至今日，雖然世衛組織確定了新冠病毒源於自然界，但對於病毒在自然界中隱藏宿主的尋找仍在路上；[6] 曾主審“馬加爵案”和參審“孫小果案”而被公眾熟知的法官刀文兵因涉嫌故意殺人罪等多項罪名，於 2020 年 5 月被雲南省高級人民法院指定審判，[7] 伸張正義、定紛止爭的司法官員也可成為背棄正義、製造紛爭的罪魁禍首。

---

[1] 史秉能：〈錢學森科技情報學術思想及其意義〉，《錢學森研究》，2018 年，第 2 期，第 74–83 頁。

[2] Namsoo Shin Hong：〈解決良構問題與非良構問題的研究綜述〉，杜娟、盛群力譯，《遠端教育雜誌》，2008 年，第 6 期，第 23–31 頁。

[3] Spiro, R.J., Feltovich, P.J., Jacobson, M.J.& Coulson, R.L., “Cognitive flexibility, constructivism and hypertext: random access instruction for advanced knowledge acquisition in Ill–Structured Domains”, Educational Technology, 05, 1991, 11–24.

[4] David H · Jonassen，〈基於良構和劣構問題求解的教學設計模式（上）〉，鐘志賢、謝榕琴譯，《電化教育研究》，2003 年，第 10 期，第 33–39 頁。

[5] 陳琦、劉儒德：《當代教育心理學》，北京師範大學出版社，2019 年，第 104–115 頁。

[6] 劉曲：〈世衛組織：新冠病毒來源調查需“以科學為中心”〉，新華網，2020 年 5 月 5 日，http://www. xinhuanet.com/2020–05/05/c_1125944230.htm。

[7] 佚名：〈刀文兵故意殺人、掩飾、隱瞞犯罪所得、犯罪所得收益、非法持有、私藏槍支、彈藥管轄刑事決定書〉，中國裁判文書網，https://wenshu.court.gov.cn/website/ wenshu/ 181107ANFZ0BXSK4/index.html?docId=fc43a82aa19f4597a444abf1009f6a6a，2020 年 7 月 7 日。

（一）非良構偵查情報存在的現實

待偵案件性質、狀態及類屬邊界等不確定性決定了偵查人員認知非良構情報的客觀現實。當偵查人員向案件知情人詢問嫌疑人面部特徵時，知情人可能回答：“短髮、大眼睛、皮膚較黑”。這些情報都是模糊性概念，從未有人給出過“短髮”、“大眼睛”、“皮膚黑”的具體資料，之前的“短髮”很可能會在日後留成“長髮”，同樣，兩個人擁有幾乎同樣大小眼睛的人，由於參照的臉盤大小不同，人們所得到的認知結果也不相同。可以說，構成案件的各子系統，人、事、物、時、空等都具有不確定性。對於一個陳屍現場，是意外事件還是犯罪所致？若存在犯罪行為，是故意還是過失？若是故意犯罪，是財殺、情殺、仇殺，還是報復社會或其他原因？是臨時起意，還是早有預謀？是本地人，還是外地人？年齡、體貌特徵、作案時間長短、使用何種工具等，這些涉案事物在案情分析初期都是模糊不清的。如果作案人為了掩蓋犯罪事實還故意製造假象，或者案發現場受到自然或人為因素干擾，將會使客觀事實更深藏於雲霧之中，給偵查人員帶來各種判斷要素均或多或少兼而有之的感知結果。再如，現場狀態是犯罪行為的外在表現，作案人從預謀、實施到後續行為，從犯罪行為引起的物質變化以及心理痕跡，在時空上都是有明確序列性的。偵查人員在進行回溯重建時不可能毫無差錯地再現犯罪過程，情節上的遺失、時間上的中斷、空間上的間隔現象都是無法避免的。這要求偵查人員必須面對和接受非良構情報，暫時放下某些不確定、不清楚的仲介聯繫，保留若干空白，根據有限的線索和信息，按照一定的策略或模型對案情及情報做出認知判斷，擬定可行的研判路徑，形成偵查決策。

（二）非良構偵查情報存在的緣由

非良構偵查情報的存在源於偵查人員實踐認識活動，而非認識物件本身。非良構並非客觀事物本身的固有屬性，事物本身無所謂良構或非良構。它也不是偵查人員主觀自生的特性，而是偵查人員在認知實踐中產生的。只有從偵查人員和認知客體的相互關係中，才能正確理解和把握非良構偵查情報的內涵。所謂非良構情報是指那些自身屬性、所處狀態及類別邊界不確定的案件信息，是由內部矛盾特殊性決定的案件性質和狀態在偵查人員面前表現出不確定性和不穩定性。當與案件有關的事物正好處於對立矛盾的“兩級”位置，而且此消彼長、此起彼伏的矛盾雙方實力對比相對均衡時，事物的自身性質、所處狀態會顯現出相對穩定性，如“非黑即白”或“非此即彼”，這類事物處於良構狀態。當與案件有關的事物正處於對立矛盾的“仲介”位置而同時兼具矛盾雙方的某些成分，很容易向此消彼長、此起彼伏的另一方遞進，它的自身性質及所處狀態就呈現出不穩定性，如黑白之間的灰色系統和彼此之間的亦此亦彼特徵，這類事物就處於非良構狀態，它們體現了對立矛盾兩級間的不均衡性。涉案事物的類屬邊界對偵查人員而言也具有不確定性。事物之間除了並列關係，還有類屬關係。偵查人員為了便於識別與案件有關的事物，總要依據一定的標準對它們進行分類，有些事物之間具有明確的界限，如賭博案件中賭資在 500 元以上或 500 元以下，偵查人員對它們的認識是良構性的。但是，在其他案件中，還有許多與案件有關的事物之間沒有明確界限，如嫌疑人文化水平的高或低，年齡偏大或偏小，屍溫是冷或暖，作案時間在白天或夜間等，它們都是處於矛盾之間的逐步過渡狀態。[8] 可以說，在由偵查人員、認知客體和認知活動三個基本要素組成的情報認知過程中，偵查人員與認知客體的絕對運動以及相互作用，是非良構偵查情報產生的客觀根源。

除了實踐認識活動的客體原因外，也有以下偵查人員的主觀因素。一是從認知條件看，偵查人員的感官具有局限性，不能直接感知事物內部，更不能毫無遺漏地深度感知呈現給感官的所有事物，如佈設於火車站等人流高度密集區域的人臉智慧識別探頭，可同時識別 2,000 人以上，這種能力是人的肉眼無法達到的。二是從認知方式看，當偵查人員孤立、靜態地勘驗案發現場的某個痕跡或物品時，容易看到其確定形態，獲得對痕跡或物品的良構情報；而當偵查人員以聯繫、動態的視角進行勘驗時，如判斷案件現場的空間結構及邊緣地區，又如推斷作案過程及時間順序等，就難以得出良構情報。往往是涉案事物之間的聯繫

[8] 李曉明：《模糊性：人類認識之謎》，人民群眾出版社，1985 年，第 12–21 頁。

越密集，認知上就越難以進行良構。三是從認知方位看，就縱向層域而言，程度越淺越易良構，程度越深越不易良構；就橫向時域而言，以當前為原點，越向前追溯或往後推移，認識越容易良構。[9] 當然，我們不能因為偵查情報非良構性的主體緣由而否認其客觀性，非良構在本質上是客觀的，是處於普遍聯繫和持續發展狀態中的客觀事物所呈現出的一種整體特性。

（三）非良構偵查情報的模糊認知

偵查人員既有嚴格縝密的精確認知能力，也有靈活高效的模糊認知能力。模糊認知是人腦思維的特點和優點，它彌補了精確認知的不足，成為現代科學方法體系中的有機組成部分。1965 年控制論專家紮德（L.A.Zadeh）吸取了社會科學領域使用的“模糊”術語，從中抽象出具有方法論意義的隸屬度和貼近度兩個原則，並以排中律的破缺為基礎發表了著名論文《模糊集合》（Fuzzy Sets），宣告了新的數學分支—模糊數學的建立。作為一種處理非良構物件的理論，它通過建立精確的數學模型，用比較簡便的方法提取關鍵指標，對非良構物件做出相對精確、切合實際的判斷，並為許多領域提供了新的研究範式和工具。由此，人們把模糊數學在各個領域的應用統稱為模糊理論。模糊認識便時常適用於類似這樣的非良構情勢。雖然偵查人員的認知物件是非良構的，但對非良構情報的模糊認知方法本身並不模糊，它通過提煉明確的分析策略或模型，用容易掌握的分析思路準確把脈認知過程的關鍵節點，對處於非良構狀態的模糊情勢做出清晰、便捷、可操作性強的認知判斷。

模糊認知能夠幫助偵查人員對非良構情報迅速做出認知判斷。偵查人員並不是對進入感官的所有案件信息都進行接收和加工，而是具有過濾功能，他要基於當前待偵案件對大量涉案信息進行篩選和提取，抓住小量反映案件法律真實的情報，濾去自己認為無關的信息，對案情形成一定的模糊概念。偵查人員通過對情報信息接收和忽略，來適應和彌補人腦相對低速運轉的實況或缺陷。在辨識涉案信息的過程中，偵查人員可以把所篩選出的案件信息與自身經驗知識和專業知識融合成高度靈活的認知圖式，憑藉這種圖式，偵查人員不需要獲取大量的精確資料，就能對案情、情勢及分析策略和手段進行模糊識別和判定。偵查實踐中，偵查人員能用相對含糊的語言進行訊問，能夠撥開層層疑團，使陷入僵局的案件“柳暗花明”，說明偵查人員在判定涉案事物或信息之間的關係時，總體並非是一一對應的同構模型，而是多一對應的同態模型，是同時態、全方位、立體化、綜合性地識別和判定與案件有關的事物和信息的。這樣才能保證偵查人員在面對非良構情報時，能夠自動適用相應的邏輯分析模型進行具有高度靈活性的認知，對案情得出具有一定可靠程度的結論，以滿足在複雜情勢中查清案件事實的需要。

與精確認知相比，模糊認知呈現出三個特點：一是靈活性，它無需遵守嚴謹的邏輯程序，允許思維在不同層級和領域的躍遷、簡化、反串等。二是簡捷性，它不需要獲取大量確鑿無疑的精確材料，就能迅速對相關情報進行接收和處理。三是由靈活和簡捷帶來的認知行為的高效率。模糊認知的這些特點，會促使偵查人員模糊認知模型的生成。模糊認知是沒有確定的規則可以遵守，並能在認知成果上給偵查人員提供新思路的認知，它本質上是一種模糊思維。可以說，模糊性思維的作用，就在於它能使偵查思維具有啟發性和創造性。概言之，模糊認知和精確認知相輔相成，在非良構情報分析過程中共同發揮作用。

三、非良構偵查情報模糊認知的思維邏輯

模糊認知的思維邏輯是偵查人員根據非良構情報的表象特徵和發展變化而自覺遵循的某種思維規律。[10] 正是這種思維規律牽引非良構情報認知的進程。當各條情報線索無法查證確實，案情分析工作止步不前，陷入進退兩難的僵局情勢時，就需要充分發揮“一策而轉危局”的突破和帶動作用，通過運用模糊認知邏輯來撥開情報分析的重重迷霧，對非良構情報中把握不準的要素特徵，主動進行模糊處理。這時旨在於撥開迷霧、走出僵局的模

[9] 熊則坤：《偵查辯證法》，警官教育出版社，1997 年，第 194–205 頁。

[10] 楊宗輝：《偵查學總論》，中國檢察出版社，2017 年，第 264–269 頁。

糊認知邏輯便使更多與案件有關的情報信息進入偵查人員的思域範圍，使非良構情報逐漸由模糊到精確。

（一）模糊認知思維的邏輯要素

1972 年西蒙和紐威爾 (Herbert Simon & Allen Newell) 因受認知心理學中信息加工取向的影響，在《人類問題解決》一書中提出了逐步搜索初始狀態與目標狀態之間路徑的問題解決策略。依據西蒙和紐威爾將認識者所面臨的待解決任務表徵為“問題空間”視域，偵查人員可將非良構情報看作為“情報空間”，一個情報空間包括一組情報狀態（初始狀態、目標狀態及各種可能的過渡狀態）、一組允許一個情報狀態運動到另一個情報狀態的運算元、情報分析人員在情報空間中選取路徑的局部要素。這樣來看，對非良構情報進行模糊認知的思維邏輯可以被概括為：手段──目的，即對貫穿於整個情報空間中的能夠連接初始情報狀態和目標情報狀態的各條路徑的搜索。

手段──目的認知思維的核心要素是發現非良構情報的初始狀態與目標狀態之間的差別，並應用運算元來縮小這種差別。以這種方式對非良構情報進行認知，還需要滿足某些條件，即消除應用運算元與當前狀態的差別，如此一步步進行下去，以逐步接近和達到目標狀態。換言之，就是將情報認知需要達到的目標分成若干子目標或子任務，通過完成一系列的情報認知子目標或子任務，最終達到總目標。[11] 它的基本步驟是：(1) 比較初始狀態與目標狀態之間的差距，提出第一個情報認知子目標；(2) 確定完成第一個子目標的策略和手段；(3) 實現情報認知子目標；(4) 提出新的情報認知子目標，如此迴圈往復，直至情報認知總目標的實現。[12] 當偵查人員對某些子目標一時難以完成時，應不惜增加困難較小的子目標或暫時擴大既有差別，以有利於完成困難較大的子目標。一般而言，偵查人員在明確了初始狀態和目標狀態之間的差別後，都會全神貫注於減少這種差別。但如果一味地尋求減少差別，有時很可能忽略掉破除疑難或突破僵局的關鍵步驟。這時，偵查人員需要在既定的認知步驟基礎上後退幾步，暫時從目標狀態移開，進行必要的迂迴，以擴大初始狀態和目標狀態之間的差異。在偵查實踐中，當遇到眼前難以逾越的非良構態勢時，最有效的偵查策略其實是暫時後退。

（二）模糊認知思維的邏輯例析

以偵查人員辦理一起侵犯商業秘密犯罪案件為例。初始狀態與目標狀態之間的差別是什麼呢？主要是兩者之間的犯罪事實清晰度，而增加清晰度的運算元便是偵查人員收集的證據。偵查人員先要對報案人提供的涉嫌侵權技術信息認定為商業秘密，怎麼才能證明涉嫌侵權的技術信息屬於商業秘密呢？委託鑑定機構進行鑑定。在確定涉嫌侵權的技術信息確實屬於商業秘密後，又如何查找侵犯商業秘密犯罪嫌疑人呢？篩查侵權行為的受益人範圍和商業秘密的接觸人範圍。在掌握了嫌疑人基本情況後，又如何確定這種侵權行為給權利人造成了重大損失呢？調查涉案企業的經營情況。用什麼辦法才能調查清楚涉案企業的經營情況呢？查詢涉案企業銀行帳戶……從這個例子可以看出，為了查清侵犯商業秘密犯罪案件並達到偵查終結狀態，需要發現初始狀態（立案）與目標狀態（偵查終結）之間的差別（犯罪事實清晰度），由此採取某種適當的方式（收集證據）來消除這個差別，使用證據這種方式需要完成一定的子目標（明確是否屬於商業秘密），在使用某種適當的措施或手段（鑑定）消除這個差別後，又出現新的子目標（查找犯罪嫌疑人），通過一些偵查步驟和手段（篩查受益人範圍和借出人範圍）消除這一差別之後，還需完成下一個子目標（造成重大損失），偵查人員通過採取偵查措施（查帳）又將差別進行消除，如此繼續進行，直到獲取確實、充分的證據來證明犯罪事實。因此，手段──目的是一種有明確方向、通過設置認知過程中的子目標來逐漸縮小初始狀態和目標狀態之間差別的模糊認知思維。

（三）模糊認知思維的邏輯擴延

與手段──目的認知思維類似的是爬山法。理解這種認知思維，偵查人員可以將偵查某個疑難案件想像

[11] 王甦、汪安聖：《認知心理學（重排本）》，北京大學出版社，2006 年，第 193 頁。

[12] 彭聃齡：《普通心理學》，北京師範大學出版社，2019 年，第 276 頁。

成自己正在一個不熟悉的地方沿着一條路爬山，目標就是到達山頂，但眼前突然出現了岔路，順着兩條路的方向看去，都無法看到太遠的地方，更無法確定哪條路能夠到達山頂。因為此時的目標是往上爬，所以你選擇了一條坡度較大、看上去離山頂更近的路。[13] 當偵查人員在模糊認知中只能夠把握到接下來的偵查措施和手段，而缺少其他可選項的必要信息時，就可以使用爬山法認知思維，但這種認知思維也可能會使偵查人員誤入歧途。這個思維邏輯最大的缺陷是，偵查人員必須一直選擇看起來可以直接通向目標的措施和手段，但並不能保證真正能夠實現目標。例如，爬山時看起來坡度較大的路有可能通向山頂，但也有可能這條路會很快走到盡頭而無法到達山頂。

爬山法或手段──目的都是很有彈性的模糊認知思維，偵查人員經常在那些不受到經驗知識或專業知識所束縛的案件中使用，並能成功解決諸多疑難問題。也就是說，儘管在面對比較新穎的非良構情報時，偵查人員一般會依賴這種認知思維，一旦偵查人員獲得有關特定情報空間的經驗或專業知識時，就會中斷這種認知思維，並且就在獲得情報空間特定知識的那一點，偵查人員開始將認知思維切換到更熟悉、更專業的思維方式上。一般而言，即使偵查人員所擁有的情報空間的一些專業或經驗知識的適用範圍比較狹窄，他們也更傾向於使用與專業或經驗知識相關的認知措施和手段。專業或經驗知識對認知思維的影響，使得偵查人員把注意力從因知識貧乏引發的非良構狀態轉變為與偵查人員經驗或專業知識相關聯的較為熟悉的良構狀態上來。因為，在那個有經驗或專業等背景知識支撐的情報空間，偵查人員往往能夠自發地使用自上而下的信息加工，更好的發揮以往經驗中獲得的知識和記憶的作用，當然，心理定勢和功能固着的影響也會不可避免的隨之而來。

手段──目的認知思維是從情報認知的初始狀態逐步接近並達到目標狀態，這可以說是一種正向認知邏輯，但在認知某些非良構情報時，也可以採用逆向搜索認知邏輯，從情報認知的目標狀態往回走，倒退到發案狀態，效果也很明顯。例如：在認知一起殺人案件時，如果按照手段──目的認知邏輯，當偵查人員調查了解到被害人曾與他人有債務糾紛時，很可能會沿着債務糾紛這條線索開展正向認知；如果按照逆向搜索認知邏輯，偵查人員通過分析和篩查對被害人死亡這一結果的潛在受益人範圍後，很可能會覺察到除債務糾紛之外的其他更多可能性。相較而言，如果從情報認知的初始狀態到達目標狀態的路徑有多條，一般用手段──目的認知邏輯能夠起到很好的效果；如果可選的路徑很少，則適宜採用逆向搜索邏輯，跳出當前非良構情報空間的束縛，尋求更多的可能性。

四、非良構偵查情報模糊認知的思維範式

有些偵查人員在情報會商中能夠把與案情有關的點點滴滴迅速串聯起來，描繪和發掘出更大圖景或更多視角，想出彌合非良構情報初始狀態和目標狀態之間差距的絕妙運算元，這種能力依賴於一種特定技能──創造性認知。一般而言，這種技能並不局限於那些具有創造力的人，很多人都可以從這種認知方式中受益，因為人類大腦有一種自然傾向，會自覺選入某種認知“捷徑”，這種“捷徑”通常表現為選擇、良構、模擬三個遞進的思維層域。

（一）模糊認知思維的選擇層域

情報認知伊始就表現出主客體之間的相互作用。所謂主體是指偵查人員、偵查人員的認知思維以及隱存偵查人員腦中的思維範式；客體是指犯罪案件、案件的外在表象以及與之相關的所有非良構特徵。在偵查人員與案件接觸之初，情報就以客觀留存形象或犯罪行為表現呈現在偵查人員的感官之下並作用於認知思維之中。例如，案件受害人以自己的陳述力求偵查人員全面了解犯罪行為造成侵害的前因後果，並試圖通過強調自身遭受的損害使偵查人員明白其報案訴求，這充分表明了客體對主體的影響。不難發現，有關案件表象的思維輸入，對偵查人員的模糊認知具有積極意義。

[13] 同註 12。

此時，偵查人員總是在觀察、聆聽、分析，試圖從與案件有關的非良構情報中搜羅出具有犯罪意義的良構性表象，甚至力求找出最具價值的典型表象以明確案件所有矛盾的集中所在。但是，案件客觀表象和被害人或知情人的相關陳述不等於偵查人員對情報要素的輸入與接納，有時某些明顯痕跡、被害人、知情人自認為重要的信息被偵查人員摒棄或放置於不太顯眼的地方，而那些不起眼的被害人、知情人，並未過多言及的內容，卻被映襯和突顯出來；當遇到試圖隱瞞案情的被害人或知情人，則更需要偵查人員去撥開迷霧、探明隱情；偵查人員亦需通過必要的勘驗尋訪和檢驗鑑定來獲取情報表象，這都顯示了主體對客體的能動選擇。總之，偵查人員在認知中輸入情報表象時不是被動消極的，而是以積極能動的姿態介入。偵查人員必須清晰地意識到有選擇的表象輸入才是真正的輸入，對於非良構情報的認知才具有意義。如果對情報表象不加以選擇，其結果不僅會使偵查人員的情報認知不得要領，不能抓住情報的主要矛盾和矛盾的主要方面，以至於使偵查人員的認知判斷出現偏頗，而且很容易使其誤入認知歧途，對非良構情報的構成要素做出錯誤判斷。可以說，偵查人員對情報表象作了偵查意義的考察、取捨後，情報表象才得以真正輸入。

（二）模糊認知思維的良構層域

偵查人員能動選擇非良構情報表象後便會開啟良構認知。實際上，偵查人員的良構認知很早就開始了，他們總是根據隱存腦中的專業知識和實踐經驗對情報表象邊選擇邊良構，直到思想上形成一個情報構成要素與犯罪嫌疑人心理畫像的整體知覺再現為止。所謂良構，它不同於情報表象的原構。原構是指情報表象的相互共存與先後有序，它一定程度地反映了案件發生、發展全過程，因而有其必然性；但這個“共存”與“先後有序”也夾雜着某些非犯罪因素，因而可能與案件自身無關而存在偶然性。這就需要偵查人員憑藉專業知識與辦案經驗去甄別、梳理出能顯示非良構情報各種表象本質聯繫的概念鏈，這就是良構。原構生乎自然，卻是朦朧的；而良構形成於人為，但卻是清晰的，它代表着偵查人員對情報諸多表象關係的理解，有助於非良構情報的精確論斷。

偵查人員對表象的選擇和良構都遵循一定認識範式的指導。範式先隱存大腦中，它是偵查人員思維選擇和良構的思想基礎。相應認知範式的有無，常常制約着偵查人員能否對非良構情報進行選擇和良構。[14] 認知範式就是人們通常所說的認知結構。在偵查人員的認知結構當中，除了專業知識外，還有立案標準、偵查措施、訴訟程序及各類案件情報的認知要領。誠然，專業知識涵蓋不同種類情報的認知要領，之所以將它強調於專業知識之外，是因為各類情報認知要領，在對非良構情報的認知判斷中，所起的模擬認知作用有別於其他範式。

（三）模糊認知思維的模擬層域

情報認知要領是既有情報的認知判斷模式，類似於修建大型建築的施工圖紙，是偵查人員對非良構情報進行認知類比時所參照的樣本。它產生於偵查人員對情報表象的把握，並隨着偵查人員辦案實踐的加深而不斷變化發展，潛移默化地定格於偵查人員的認知思維中。因此，每個偵查人員的頭腦中都有些認知要領存在，而差異僅在於各類認知要領的成熟度與數量上的多寡而已。情報認知要領的構成以犯罪構成標準為其核心內容，因而是理性的；可它又印嵌着偵查人員個人對所經手過的情報表象的深刻印跡，於是又是感性的。所以，每當面對類似情報的相關表象時，它即從思維深處彈跳而出啟迪和引導着偵查人員迅速做出認知判斷。可以這麼認為，以犯罪構成要件模擬情報表象，主要是抽象思維在起作用，而以各類情報認知要領模擬情報表象則還要借助於形象思維發揮作用。情報認知要領和純理性的犯罪構成要件的不同之處還在於，犯罪構成要件為每個偵查人員所遵循，它是共有的；而情報認知要領則成熟於偵查人員的辦案實踐，凝結着偵查人員的經驗，且因偵查人員的情報際遇不同而有所區別，並且偵查人員的實際認知行為與規範性的理論模型之間必然存在着無法忽略的差異，[15] 因而是偵查人員個人的，在每次認知中都能顯示出

[14] 周三多、陳傳明、魯明鴻：《管理學——原理與方法》，復旦大學出版社，2009 年，第 247–252 頁。

[15] 丹尼爾·卡尼曼 (Daniel Kahneman)、阿莫斯·特沃斯基 (Amos Tversky)：《選擇、價值與決策》，鄭磊譯，機械工業出版社，2018 年，第 218–220 頁。

偵查人員個人在認知進程上的獨到之處。

非良構情報的模糊認知離不開良構基礎上對犯罪構成要件或情報認知要領的模擬認知。比如，經過偵查人員整理出的某類犯罪情報之表象是十餘人經常糾集在某地稱霸作惡、以暴力手段敲詐勒索群眾、實行強買強賣、賄賂基層官員、聚斂錢財、放高利貸……而偵查人員又判斷該案件屬於黑社會性質組織犯罪，就有了情報表現之良構與黑社會性質組織犯罪構成要件及情報認知要領相模擬的認知過程。概言之，我們可以將非良構情報認知中對情報表象的選擇、良構與類比看成是模糊認知進程的“三步曲”，一步一趨地“篩選”出了非良構情報的認知判斷。

五、結語

非良構情報認知是一個模糊認知的過程，其遵循的思維邏輯是手段──目的，而內隱的邏輯範式可概括為選擇、良構、模擬三個遞進層域。上述研究結果，有助於強化偵查人員對非良構情報的發掘和運用，有助於提升非良構情報向良構情報的轉化，有助於實現非良構情報認知的便捷性。偵查人員應充分拓展模糊認知的功能，使其不僅在非良構情報認知領域發揮作用，還可在大數據智慧情報分析等領域發揮可貴價值。

試論澳門招工詐騙犯罪的現狀及對策

李錦添 *

摘要：在全球化趨勢下，各國的經濟貿易關係日漸緊密，對人力資源的需求越趨殷切，勞動人員異地就業、網上就業的情況十分普遍。澳門自回歸祖國後，實行賭權開放政策，以博彩旅遊產業作為澳門經濟的重要支柱，職位空缺數量遽增；然而，本地勞動力增長速度未能滿足人力市場需要，企業商戶遂將目光轉移至境外高技能專業人才及低端勞動力，以優於其原居地的薪酬水平吸納他們來澳就業，澳門特區政府亦制定相關法律法規，以規範聘用外地僱員制度，保障勞資雙方的權益，並促進澳門經濟社會的良性發展。因此，共同預防和打擊跨境勞務犯罪活動，確保本地居民和外來勞動人員的財產安全，是海峽兩岸和港澳警方永不停步的工作。

關鍵詞：勞動人員　跨境勞務犯罪　安全　合作模式

A Brief Discussion on the Situation of Recruitment Fraud and the Countermeasures Against this Crime in Macao

Lei Kam Tim

Abstract: Under the trend of globalization, the economic and trade relations between countries have become increasingly close, and the demand for human resources has become stronger and stronger. Working away from home and working online is very common among workers. Since its return to the Motherland, Macao has been following an open policy towards the gaming industry. Gaming tourism has become an important support of Macao's economy and the number of job vacancies has thus increased rapidly. However, the growth rate of the local labor force has failed to meet the needs of the labor market, and so enterprises and businesses turn their attention to those high-skilled professionals as well as those low-skilled labor outside Macao. They offer them wages that are better than what are being offered in their hometown to attract them to come to Macao to work. The Macao SAR government has also formulated relevant laws and regulations to regulate the employment system of foreign employees in order to protect the rights and interests of both employers and employees, in addition to enhancing a healthy economic and social development in Macao. Therefore, aside from preventing and combating cross-border labor-related crimes together, ensuring the safety of both local residents' and foreign workers' properties is also a never-ending task of the cross-strait police, the Hong Kong police and the Macao police.

Keywords: Workers; Cross-Border Labor-Related Crimes; Safety; Cooperation Modes

*　李錦添，司法警察局經濟罪案調查處首席刑事偵查員。

一、前言

澳門回歸祖國以來，在中央政府大力支持下全力發展經濟，其中包括簽署《內地與澳門關於建立更緊密經貿關係的安排》（簡稱 CEPA）、受惠於開放港澳自由行政策、簽訂《粵澳合作框架協議》等等，推動澳門可持續發展。2002 年，澳門開放幸運博彩經營權，並以博彩旅遊產業作為澳門經濟的重要支柱，外資博企相繼進入澳門市場，與之相關的基礎建設、餐飲及零售業亦出現井噴式發展，職位空缺數量遽增；然而，本地勞動力增長速度未能滿足人力市場需要，企業商戶遂將目光轉移至境外高技能專業人才及低端勞動力，以優於其原居地的薪酬水平吸納他們來澳就業，間接提升澳門各行各業的薪酬福利水平。與此同時，隨着網絡科技高速發展，網上工作日漸盛行，亦帶動了一批無法在崗工作的勞動力重新投入職場。在這種情況下，職業介紹服務、網絡招工等成為人們求職的窗口，犯罪分子窺準人們不熟悉招聘程序及求職心切的心理，設法從中牟取不法利益，衍生的招工詐騙犯罪時有發生。本文嘗試以職業介紹服務及網絡招工相關的犯罪情況為視角，對不同地方的執法部門創新和制訂合作模式、共同預防和打擊相關犯罪進行思考。

二、澳門外地僱員概況

（一）澳門輸入外地僱員的背景

基於歷史發展的特殊性，澳門很早便成為了國際貿易的重要中轉港，於二十世紀 70 年代後期，以紡織業、製衣業為主體的經濟結構開始興盛，至 80 年代進入發展全盛時期，由於該等行業的工作環境及待遇條件不佳，造成當時勞動力非常緊張，澳葡政府接納商人建議，從 1984 年開始大量輸入外地勞工（尤其是從中國大陸），[1] 並於 1988 年對外勞輸入作出法律規範。自此，澳門外地僱員數量逐年遞增。

根據澳門統計暨普查局及勞工事務局的資料顯示，截至 2023 年第三季，澳門總人口約 681,300 人，其中外地僱員共 171,744 人，佔澳門總人口近四分之一。澳門的外地僱員來自世界各地，如中國、菲律賓、印尼、越南、尼泊爾、緬甸等，其中來自中國大陸的外地僱員最多，佔澳門總體外地僱員人數 70.65%，至於來自香港特區及台灣地區的外地僱員分別佔澳門總體外地僱員人數的 1.44% 及 0.34%。（見圖 1）

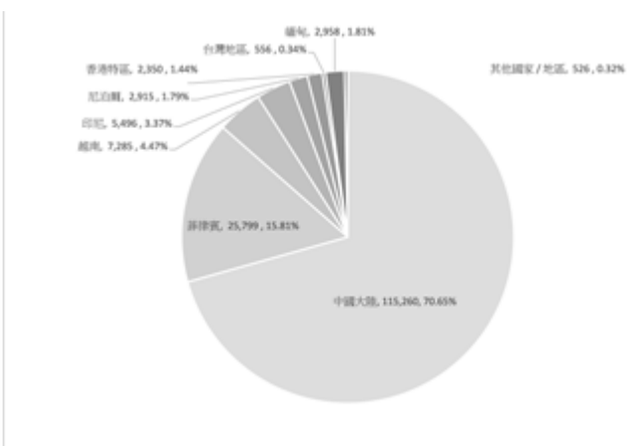

圖1　2023年第三季澳門外地僱員人數統計（按身份證明文件發出國家 / 地區分類）[2]

（二）澳門外地僱員的待遇

根據澳門經第 10/2020 號法律修改的第 21/2009 號法律《聘用外地僱員法》第三條的規定，外地僱員可受聘為：1. 專業僱員，如受聘者具備高等教育學位，又或具備高度技能或專業工作經驗，且為履行具高度專業要求的工作；2. 家務工作僱員；3. 非專業僱員，如受聘者不具備上述專業外地僱員的要件，且非為提

[1]　米健等：《澳門法律》，澳門基金會，1994 年，第 316 頁。

[2]　澳門勞工事務局，網址：https://www.dsal.gov.mo/download/pdf/statistic/nrworker/A1/A1_2023_09.pdf，到訪日期：2024 年 1 月 30 日。

供家務工作。基於三類僱員可從事的行業對學歷、語言及工作經歷的要求並不一致，加上各行業的工資水平有所差異，本文以澳門統計暨普查局公佈的相關資料，整理出部分行業的外地僱員平均工資數據，以作參考。(見圖 2)

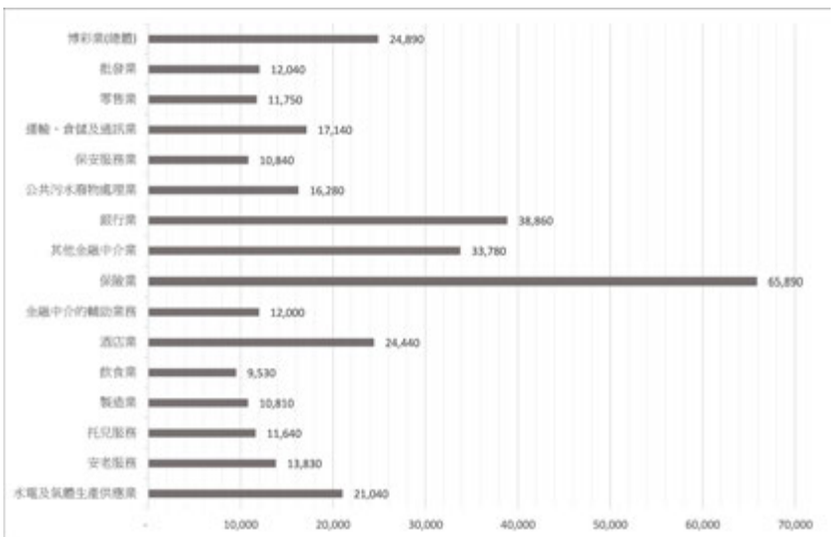

圖2　2023年第二季及第三季澳門部分行業外地僱員平均工資 (單位：澳門元) [3]

外地僱員除了領受工資外，還可按《勞動關係法》及受聘公司規章制度，享有休息時間、每周休息日、強制性假日、年假、合理缺勤及其他保障的權利。綜上可見，澳門優厚的工資及完善的福利保障制度，是外地居民樂於來澳就業的主要誘因。

(三)外地居民到澳門工作的條件

經第 10/2020 號法律修改的第 21/2009 號法律《聘用外地僱員法》、第 8/2010 號行政法規《聘用外地僱員法施行細則》及第 13/2010 號行政法規《規範聘用外地僱員許可內設定的條件或負擔》共同構成澳門特區輸入外勞的法律規範。目前，澳門特區政府輸入勞動力政策的大前提是確保本地僱員優先就業及勞動權益不會受損，只有在本地人力資源缺乏或不合適時，才會考慮輸入外地僱員作為臨時補充。輸入外地僱員的申請必須由僱主（自然人或法人）向勞工事務局聘用外地僱員廳提出，經取得聘用許可後由僱主直接或透過獲發准照的職業介紹所招募僱員。一般情況下，外地居民到澳門工作，除了與僱主簽訂勞動合同外，還須取得澳門當局發出的工作許可。審批外地僱員在澳門的工作許可屬勞工事務局的職權範圍，而批准外地僱員進入及逗留澳門則屬治安警察局的權限。僱主必須為獲准輸入的外地僱員申請《外地僱員身份認別證》（簡稱“外地僱員證”或“藍卡”）。有關申請可由僱主或其合法代理人，或透過澳門法定的職業介紹所向治安警察局居留及逗留事務廳外地僱員分處遞交。

此外，倘若中國大陸居民欲赴澳門工作，必須通過中國大陸居民赴澳勞務經營公司[4]辦理勞務手續，澳門僱主或其他中介機構也不能直接到中國大陸招聘勞工。中國大陸居民赴澳門特區工作前必須簽訂兩份合同，即《赴澳門特別行政區勞務派遣合同》和《外地僱員輸入申請之勞動合同》，前者由勞務人員本

[3]　澳門統計暨普查局，網址：https://www.dsec.gov.mo/zh-MO/Statistic?id=302，到訪日期：2024 年 1 月 30 日。

[4]　內地對輸澳勞務管理主要依據《商務部國務院港澳辦中央政府駐澳門聯絡辦關於內地輸澳勞務管理體制改革的通知》(商合發 [2003]262 號，簡稱《通知》)。根據《通知》，商務部會同港澳辦，徵求中聯辦的意見後，核定內地對澳門特區開展勞務合作業務經營公司的名單。目前，經核定的內地公司共 19 家，分別是：廣東新廣國際集團有限公司、江門市對外勞動服務公司、莆田市國際經濟合作有限公司、中國國際技術智力合作公司、福建中福對外勞務合作有限公司、福建省對外勞務合作公司、中國廣州國際經濟技術合作公司、珠海對外勞務合作有限公司、漳州國際經濟技術合作公司、中國廈門國際經濟技術合作公司、珠海國際經濟技術合作公司、上海市對外勞務經貿合作有限公司、泉州中泉國際經濟技術合作 (集團) 有限公司、中國南光進出口總公司、廣州對外經濟發展總公司、中國福州國際經濟技術合作公司、中國成套設備進出口 (集團) 總公司、中國鐵道建築總公司、北京外航服務公司。見澳門貿易投資促進局，網址：https://www.ipim.gov.mo/zh-hant/mainland-china-business-qa-tc/ 勞務輸出入 /，到訪日期：2024 年 1 月 30 日。

人與勞務經營公司簽訂，後者則由勞務經營公司負責協助勞務人員本人與僱主簽訂。同時，中國大陸勞務人員赴澳前應參加外派勞務人員培訓及考試、辦理體檢並領取《國際旅行健康證明書》。相關赴澳勞務的證件及簽注手續由勞務經營公司負責辦理，勞務人員需負擔中國內地公安部門規定的證件及簽注工本費。[5] 至於香港特區和台灣地區的居民則可自行向澳門僱主或透過澳門的中介機構協助申請而取得澳門當局發出的工作許可。

（四）澳門外地僱員的行業分佈

澳門以博彩旅遊業為主體產業，配合製造業、金融保險業及建築地產業，成為澳門的主要行業。澳門回歸祖國後，中央政府根據澳門《基本法》全面落實“一國兩制”、澳人治澳和高度自治的發展方針，大力支持澳門經濟發展，而自賭權開放後，更使澳門經濟急速騰飛，一些勞動條件差、工作時間長、工資水平相對較低的行業，例如：餐飲服務員、清潔工人、保安員、建築工人等等的低技術高勞動力的工種缺乏人手，為了穩定就業市場需求，維持澳門的經濟發展，澳門特區政府輸入外地勞工以填補相關勞動缺口。此外，由於澳門大多數是雙職家庭，且需輪班工作的家庭為數不少，使澳門居民對家務工作僱員的需求大大提升。由於澳門的工資水平相對鄰近地區為高，吸引一些高學歷的外地勞工來澳從事上述工種。

根據澳門勞工事務局統計資料顯示，2023 年第三季於澳門工作的 171,744 名外地僱員中，以從事酒店及飲食業者最多，達 47,116 人，佔總人數 27.43%；其次是建築業，共 30,139 人，佔總人數 17.55%；第三位是家庭傭人，共 24,992 人，佔總人數 14.55%。（見圖 3）

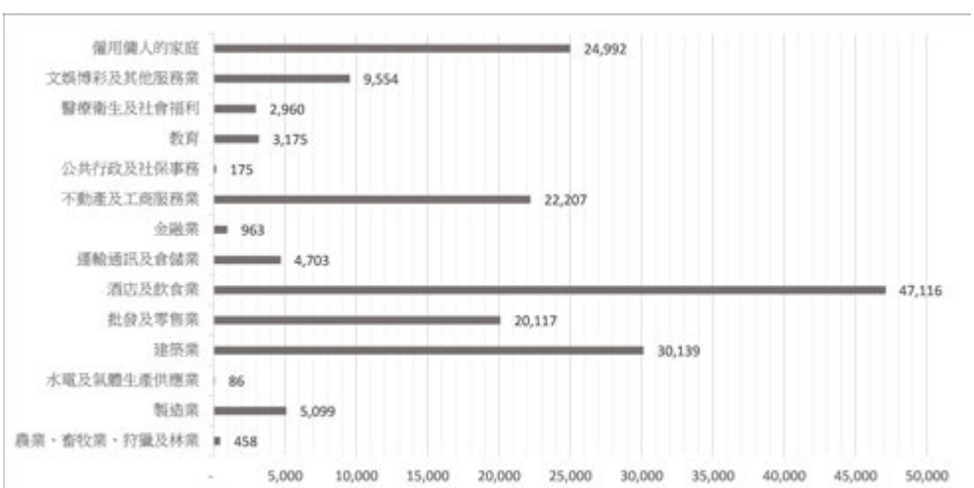

圖3　2023年第三季澳門外地僱員從事行業分佈[6]

（五）澳門對外地僱員的保障

根據經第 10/2020 號法律修改的第 21/2009 號法律《聘用外地僱員法》及相關法規的規定，為了保障外地僱員，澳門特區政府要求僱主與每一僱員以書面方式訂立勞動合同，有關勞動合同亦必須遞交澳門勞工事務局進行審批。外地僱員根據勞動合同所享有的權益和福利，不應低於澳門有關勞工法例所訂明的標準，倘未能享有合同列明的權益和福利（包括醫療、住宿等），或與僱主發生勞務糾紛時，澳門勞工事務局會提供免費的調解服務，以協助勞資雙方達成和解；如未能透過調解獲得解決，澳門勞工事務局會將有關個案轉介檢察院，並按《勞動訴訟法典》規定由檢察院代表僱員向僱主提出申訴，或由外地僱員根據《民

[5] 按照國家政策以及勞務人員與勞務經營公司簽訂的《赴澳門特別行政區勞務派遣合同》的有關規定，勞務人員應向勞務經營公司繳納服務費，標準為不超過在澳門工作合同工資總額的 12.5%。

[6] 數據來源：澳門勞工事務局，網址：https://www.dsal.gov.mo/download/pdf/statistic/nrworker/A2/A2_2022_T1.pdf，到訪日期：2024 年 1 月 30 日。

事訴訟法典》的規定提出民事訴訟程序。

目前，在澳門特區生效的國際勞工組織公約共有 34 個，[7] 而《國際勞工組織章程》亦自 1999 年 12 月 20 日起適用於澳門。這些國際規則在澳門的適用，加上澳門本地制定的勞工法例，構建了一套勞工保障法律體制。

三、在澳門發生的以外僱招工為幌子的詐騙犯罪概況（接觸式）

正如上文所述，澳門自開放幸運博彩經營權後，經濟騰飛發展，帶動勞動力需求大幅增加，然而，本地人力資源長期緊絀，大型企業特別是博企不惜以高薪招人，使人才向大型賭場酒店傾斜；隨着賭場酒店規模不斷擴大，與之相關的中小微企數量日益增加，輸入外地僱員成為支撐澳門人力資源發展的唯一出路。鑑於澳門外地僱員工資水平普遍較高，使大量外地居民心儀到澳門工作，不法分子遂以介紹到澳門工作或辦理澳門工作證為餌行騙，導致相關詐騙侵財案件時有發生。

（一）外僱招工詐騙案相關數據

本文是以澳門 2014 年至 2023 年的招工詐騙案數據作為研究基礎，涵蓋了新冠肺炎疫情前後的犯罪數字變化。

1. 立案數字

根據澳門保安司統計資料顯示，2014 年至 2023 年藉介紹工作或辦理證件詐騙案件合共 457 宗，其中以 2019 年最多，全年立案 107 宗。從案件數字來看，外僱招工詐騙案件處於平穩多發情況。值得留意的是，自 2020 年初新冠肺炎疫情爆發，年內案件數量驟降，但隨着澳門疫情防控工作奏效，外地居民赴澳工作機會增加，由 2021 年開始相關案件數量再次呈上升趨勢。（見圖 4）

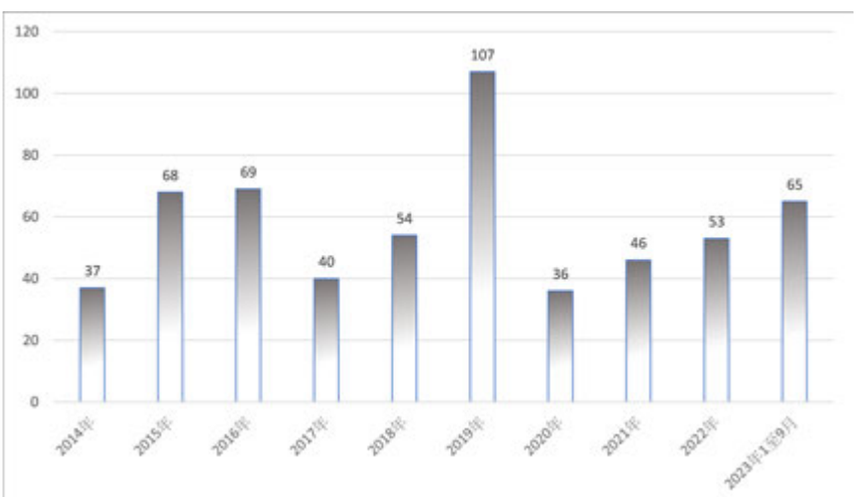

圖4　2014年至2023年1至9月藉介紹工作或辦理證件詐騙案件統計[8]

[7]　包括：1.《限定工業企業中一天工作八小時和一周工作四十八小時公約》；2.《在工業中僱用年輕人夜間工作公約》；3.《工業企業中實行每周休息公約》；4.《工人的意外事故賠償公約》；5.《工人的職業疾病賠償公約》；6.《本國工人與外國工人關於事故賠償的同等待遇公約》；7.《海員協議條款公約》；8.《海員遣返公約》；9.《制訂最低工資確定辦法公約》；10.《航運的重大包裹標明重量公約》；11.《強迫或強制勞動公約》；12.《船員膳食與餐桌服務公約》；13.《船上廚師職業資格證書公約》；14.《一九四六年最後條款修訂公約》；15.《工商業勞動監察公約》；16.《結社自由和保護組織權利公約》；17.《職業介紹設施公約》；18.《船員住房公約（1949 年修訂）》；19.《組織權利和集體談判權利原則的實施公約》；20.《對男女工人同等價值的工作付予同等報酬公約》；21.《廢除強迫勞動公約》；22.《在商業和辦公室中實行每周休息公約》；23.《國家海員身份證書公約》；24.《關於就業和職業歧視的公約》；25.《保護工人以防電離輻射公約》；26.《商業和辦事處所衛生公約》；27.《就業政策公約》；28.《准予就業最低年齡公約》；29.《三方協商促進履行國際勞工標準公約》；30.《保護工人以防工作環境中因空氣污染、噪音及震動引起職業危害公約》；31.《勞動行政管理：作用、職能及組織公約》；32.《職業安全和衛生及工作環境公約》；33.《建築業安全和衛生公約》；34.《禁止和立即行動消除最惡劣形式的童工勞動公約》。

[8]　數據來源：澳門保安司司長辦公室，網址：https://www.gss.gov.mo/cht/statistic.aspx，到訪日期：2024 年 1 月 30 日。

2. 涉案金額

根據筆者過往處理的本澳案件顯示，2014 年至 2023 年期間因外僱招工詐騙造成的經濟損失接近約 3,200 萬澳門元，其中以 2019 年最多，合共損失超過 780 萬澳門元。雖然招工詐騙案的涉案金額不及電話詐騙或其他網絡詐騙案，但以傳統接觸式經濟犯罪來看，所造成的經濟損失算是巨大，亟需各方予以重視，並積極尋求遏制之法。

（二）外僱招工詐騙犯罪手法

藉介紹工作或辦理外地僱員證進行詐騙的犯罪，是一種傳統經濟犯罪。作案人利用被害人文化水平較低及渴望賺取高額工資的心理，訛稱有能力在短時間內安排被害人到澳門的餐廳、酒店、賭場、地盤等工作，為了博取被害人的信任，作案人會要求被害人準備應聘資料，包括被害人當地身份證、旅遊證件、相片、銀行存摺、結婚證明等等，部分更會相約被害人進行面試，令被害人深信對方是真實招聘而繳付數千元不等的介紹費，隨即捲款失聯。

此外，一些“黑中介”[9] 還會吹噓已取得澳門某公司委託招聘外勞人員，向欲求職的被害人保證能安排在澳門工作，繼而要求被害人付費參加各類培訓課程，然後以不同藉口拖延，甚至失去聯絡，此時被害人才知悉受騙。

根據澳門《刑法典》第二百一十一條的規定，詐騙是指“意圖為自己或第三人不正當得利，以詭計使人在某些事實方面產生錯誤或受欺騙，而令該人作出造成其本人或另一人之財產有所損失之行為。”換言之，實施此類犯罪，必然要對被害人實施詭計，令被害人誤信作案人是有能力提供前來澳門工作的機會，從而令自己造成錢財損失。在澳門，實施詐騙犯罪最高可被科處十年徒刑。

（三）外僱招工詐騙案發的成因分析

經分析澳門司法警察局破獲的外僱招工詐騙案，大致有以下特點：

1. 作案人營造朋友關係進行詐騙

作案人一旦鎖定作案對象，一般會設法與其成為朋友，並在閒談間不經意透露自己有門路協助他人到澳門工作；被害人考慮到與作案人的個人交情，加上憧憬作案人在澳門的人脈關係，誤信作案人真誠地協助被害人到澳門工作，於是在未經查證真偽的情況下，毫無戒心地交付“中介費”、“辦證費”、“勞務費”等款項，最終墮進騙局。

案例：

2021 年 6 月，一名澳門男被害人經朋友介紹認識一名澳門男子羅某，其聲稱有能力介紹他人到澳門某餐廳任職內地外僱，但每名申請者需向羅某支付數萬元人民幣中介費，還需先繳納辦證費，可於事成後再支付餘款，並遊說被害人可協助廣傳轉介以賺取報酬，為此，被害人先後介紹合共 12 名內地人士向羅某申請有關外僱工作，以及向羅某繳付合共 17.4 萬元人民幣後，羅某最終未有按承諾期限為各申請者辦理澳門工作證，被害人懷疑被騙向澳門司法警察局報案求助。司法警察局經調查取證後，羅某承認為了獲取金錢賭博，於是對被害人訛稱有途徑協助內地工人到澳門工作，並訛稱給付介紹報酬作利誘，從而作出相關詐騙行為，贓款皆已輸光。

2. 作案人利用人們貪圖便捷的心理進行詐騙

根據《商務部國務院港澳辦中央政府駐澳門聯絡辦關於內地輸澳勞務管理體制改革的通知》，中國大陸居民如欲申請來澳工作，必須透過內地對澳門特區開展勞務合作業務經營公司協助辦理相關手續，當中涉及若干程序，處理需時。作案人利用被害人不熟悉申請來澳工作的程序，例如作案人會訛稱與在職的澳門公司老闆相熟，並獲老闆授權負責招聘勞工，只需求職的被害人交付辦證費便可在短期內獲得聘用，所有辦理手續由作案人包辦，以此向被害人作出虛假保證，由於作案人的確是澳門公司的員工，使被害人認為對方

[9] “黑中介”是指那些沒有合法經營許可的人士或職業介紹所。

可信，更因不熟悉申請赴澳工作手續，以為作案人可提供更加便捷的途徑，從而節省一些等候時間，於是便墮入圈套。

3. 被害人親友關係形成輻射效應

作案人為求將詐騙得利最大化，會遊說被害人將招工事宜廣傳身邊親友，由於來澳工作機會難得，被害人也樂意向親友轉述有關消息，親友又會向身邊朋友、親屬口口相傳，造成更多人向作案人付款應聘。事實上，除了首名被害人因相信作案人而受騙外，其他連帶的被害人都是由首名被害人及其親友引起，彼此之間具有直接或間接的交情，往往未能及時洞悉騙局，形成由點到線、再由線到面的輻射效應，結果衍生一定規模的被害人群，於 2015 年由司法警察局破獲的一宗招工騙案中，由於各被害人都是親朋好友以及為同鄉關係，在輻射效應下，該宗騙案被害人達 200 多人，涉案騙款達 150 多萬澳門元。

4. 作案人偽造文件蒙騙被害人

不法分子為求取信於被害人，會訛稱取得澳門某企業或工程的招工委託，更會出示偽造的委託文件來增加可信性。以澳門司法警察局於 2021 年 12 月偵破的一宗招工詐騙案為例，嫌犯謊稱承接路氹城區某娛樂場泥水工程及九澳某大型工程兼取得飯堂經營權，並向被害人及其親友出示偽造的澳門真正承建商的蓋章和合同，騙取被害人等 160 人的證件及合共 40 萬元人民幣的辦證費；司法警察局接報調查，並拘捕嫌犯，以詐騙（相當巨額）罪及偽造文件罪將之移送檢察院偵辦。由此可見，一宗招工詐騙案，牽涉的被害人數實在不容小覷。

（四）外僱招工詐騙衍生其他違法犯罪活動

作案人為了能成功騙取被害人信任，往往會要求被害人交付證件、相片、銀行帳戶資料、存摺等個人資料文件，讓被害人深信作案人真正協助辦理相關手續。然而，當作案人取得被害人的個人資料後，有可能會將之轉賣予其他不法分子，造成被害人將來有機會遭遇詐騙或其他類型的犯罪。

四、在澳門發生的以網絡實施的招工詐騙犯罪概況（非接觸式）

隨着網絡科技高速發展，人們日常生活離不開互聯網，網上工作日漸盛行，網絡招聘成為了人們求職的重要途徑，帶動了一批無法在崗工作的勞動力透過網上工作重新投入職場。不法分子利用互聯網的廣泛性、滲透性、隱蔽性等特點，逐步發展出非接觸式的招工詐騙犯罪模式，以達到騙財的目的。

（一）網絡招工陷阱種類及特點

不法分子通過網絡、手機短信發佈虛假招工信息，以“彈性工作時間”、“高薪厚職”和“搵快錢”等字眼作招徠，引誘求職者陷入網絡兼職“刷單”、[10] 付費入職等騙局（見圖 5）。很多求職者求職心切，或貪圖便捷，又或被高薪厚利的招聘廣告迷惑，成為被詐騙的對象，墮入了招工陷阱，有的引致金錢損失，有的甚至被限制人身自由，被強迫參與傳銷、電訊詐騙等犯罪活動。網絡招工騙案持續高發，現時最流行的網絡招工騙案手法是“刷單”詐騙，不法分子利用被害人欲“輕鬆賺錢”的心理，以“小額返現”、“高額回報”為幌子，利誘被害人投入真實資本，最終實施詐騙犯罪。

[10] “刷單”是指以作假方式提高銷售量及商家信譽，空賣空買，不需要實際購買的行為。

圖5　不法分子透過網絡或手機短訊發佈虛假招工資訊[11]

1. 作案手法

不法分子透過手機短訊或網絡社交平台（如抖音、Facebook、Instagram、微信、微博等）發佈招聘廣告、發送短訊、直接加為好友，以“高薪”和“輕鬆”等賣點來引起被害人注意。及後，不法分子謊稱用“刷單”方式來推高商家商品銷量和人氣，要求被害人登入指定網站，購買一定數量的某款商品並墊付貨款，便可在完成“刷單”後，馬上取回貨款及收到佣金報酬。為了使被害人深信不疑，起初不法分子會馬上退回貨款及給付報酬，或在被害人的註冊帳號內顯示回佣金額，從而令被害人覺得有利可圖而繼續“刷單”，後來便會以“繳付保證金”、“升級會員”、“卡單”等各種藉口拒絕支付貨款和酬勞，並慫恿被害人必須不斷“刷單”才能拿回之前的貨款或酬勞，又發送偽造的他人“刷單”收益和付款截圖來推動被害人繼續付款；最終被害人發現受騙，騙徒卻早已失聯逃責。

2. 輻射效應更強，致被害人倍增

不法分子誘騙被害人“刷單”並成功返現來取信於被害人，隨後慫恿被害人向親友展示相關獲利紀錄，以推薦他們加入“刷單”行列；親友們則基於對被害人的信任而放鬆警惕，紛紛參與“刷單”工作。騙徒利用輻射效應成功吸納一定規模的被害人群，並引導他們增大“刷單”金額及推薦更多人工作，直到有被害人因收不到報酬而提出疑問時便立即失聯。綜觀整個詐騙過程，首名被害人是騙局的宣傳棋子，其他被害人基於信任首名被害人而被騙，事後定當會對首名被害人作出聲討，部分可能會誤以為首名被害人為騙徒同黨而報警追究，至此，騙徒既騙了錢財，也能成功把風險轉嫁到其他人身上。

（二）澳門網絡“刷單”招工騙案的情況

網絡“刷單”招工騙案於 2021 年 12 月開始於澳門湧現，在新冠肺炎疫情下澳門經濟受到衝擊，失業率上升，放無薪假的僱員增多，居民留家時間長，受到疫情和家庭經濟雙重困擾下，居民求職若渴，對網絡詐騙的防範意識減弱，加上網絡“刷單”工作標榜的“在家工作”，點擊便可獲“返利”，導致此類騙案逐漸高發。

根據澳門司法警察局的數據顯示，於 2021 年至 2023 年網絡“刷單”招工騙案立案 212 宗，涉及騙款約 1,200 萬澳門元，其中，2022 年 4 月 13 日至 19 日短短一個星期內，司法警察局共接獲 11 宗“刷單”招工詐騙案，合共損失近 120 萬澳門元，其中一人報稱損失約 33 萬澳門元。[12] 相關被害人均被網上“兼職刷單”廣告吸引，為賺取日薪 400 至 800 元人民幣及佣金，被害人通過“客服”提供的連結購買貨品，再墊

[11]　圖片來源：澳門司法警察局微信帳號“司警教室”帖文，《只需手機，立即開工！近期最火的兼職門路，原來是詐騙？》，2022 年 4 月 1 日。

[12]　〈十一人網上刷單被呃百二萬〉，《澳門日報》，第 A05 版，2022 年 4 月 21 日。

支貨款轉帳到“客服”指定帳戶，起初獲退回本金及取得佣金報酬，但其後不停被遊說加大購買金額，最終“客服”以事主操作錯誤及超時等不同藉口拒絕退款，最終失聯，事主驚覺被騙，報警求助。

五、預防及打擊招工騙案的跨境警務合作建議

正如上文分析，與澳門相關的職業介紹服務或網絡招工詐騙犯罪越趨嚴重，犯罪模式由傳統接觸式犯罪，逐漸轉向透過網絡實施的非接觸式犯罪，因此引致輻射效應，造成被害人數眾多、損失金額巨大。雖然中國內地、港澳特區、台灣地區為四個互不隸屬的獨立法域，使我國成為一個“一國兩制四域”的多法域國家。可喜的是，海峽兩岸及港澳警方長期以來採取務實合作，以各自法域居民利益為依歸的積極態度，同時相互尊重不同法域刑事法律的獨立性，秉持互惠互利的原則，基本上形成一種區際警務合作模式，相信能夠共同推進預防及打擊招工詐騙犯罪的合作。因此，本文建議從不同層面加強跨境警務合作，防止不法分子伺機侵害勞動人員的財產，保障個人財產安全。為了更有效預防及打擊此類犯罪，筆者提出幾點構想方案：

（一）架設針對勞務犯罪的情資互享平台

招工詐騙是基於求職者不熟悉異地的勞務申請情況，未能了解相關申請流程和進度，因而被犯罪分子有機可乘所致。建議相關的警務部門主動與各自的勞務部門合作，在合乎自身的法律法規下，以海峽兩岸及港澳警務合作與交流平台機制[13]作為橋樑，及參照《海峽兩岸共同打擊犯罪及司法互助協議》第八條規定“受請求方在不違反己方規定前提下，應儘量依請求方要求之形式提供協助”，以“犯罪行為地管轄”作為通用適用原則等既有的合作基礎作為切入點，構建一個具權威性的預防和打擊針對異地勞務人員的犯罪信息通報平台（下稱平台）。

有關平台必須從數位化、智慧化的方向來構建互聯渠道，並由參與方警務部門各自的經偵、技偵等相關警務部門作為平台成員以便進行對口協助，讓各方警務部門能便捷地將自身地的勞務部門有關信息分享，亦可透過平台直接與對方勞務部門聯絡，讓各方能快速地掌握對方最新的勞務信息，有效避免了繁瑣的公文往來程序；平台亦可設計將報案者提供的證據資料互享，若具管轄權的執法部門認為有需要，可在平台上作出請求，以便被請求方可即時處理，請求方亦能迅速和更好地作出相關調研和部署，大大提高執法效率。有關合作平台充分發揮科技強警的效能，使四地警務部門從被動快速反應向主動防控轉變，實現集情報、預警、指揮、行動、保障於一體的合作機制。

（二）線上線下聯動宣傳，提高求職者防騙意識

充分運用互聯網和移動互聯網的滲透性，於求職高峰期間在線上開展聯合防罪宣傳，教育民眾往外地機構求職的正確渠道信息；四地警方可在情資互聯的基礎上，將從線上獲得的勞務犯罪警情作出分析，針對容易墮入招工詐騙的群體開展線下常態化和廣泛化的反詐宣傳和精準勸阻，在合規的招工渠道上營造濃厚的宣傳氛圍，廣泛地進行防詐宣傳教育、推送招工詐騙案例，務求讓接收防騙信息的市民協助推發至身邊親友，親友又將防騙信息廣傳，使能形成正面的輻射效應，並鼓勵市民通報可疑的招工中介人及職業介紹所，一方面可令警方部門收集情報，透過上述情資平台共享，有利各地警方部署打防策略；一方面可增強警民互信，從而震懾潛在的不法分子。

（三）與銀行業界合推防騙反詐措施

網絡“刷單”及同類網絡招工詐騙與電訊詐騙作案手法，均屬於非接觸式詐騙犯罪，被害人墮入騙局後，都是按照騙徒指示透過網銀匯款至外地的銀行帳戶，款項迅速被騙徒轉移，被害人最終血本無歸。為有效減低騙款轉至騙徒帳戶的機會，可借鑑澳門司法警察局在 2019 年 7 月與澳門銀行業界實行的“可疑匯款勸退措施”，由銀行職員即時對潛在被害人作出提醒及勸阻，在櫃員窗口和 ATM 機張貼網絡詐騙宣傳海

[13] 包括《海峽兩岸共同打擊犯罪及司法互助協議》、粵港澳三地警方刑偵主管會議、滬澳警務合作會晤、粵澳警務聯絡工作會議、粵港澳警方刑事技術部門對口業務交流會。

報，又或在網上銀行和手機銀行上，在轉帳和匯款的按鈕附近，以醒目的防騙字句提醒被害人轉帳前須小心審視該項交易是否存在詐騙。此外，四地警方將作案收款帳戶透過情資平台分享，該帳戶所在地警方可立即向當地銀行通報，延緩該帳戶的到帳時間，藉此做到當下一位被害人向該帳戶匯出款項時有機會成功退匯，盡力挽回損失，而調查方亦可增加請求調查和證據調取的時間。

（四）加強與網絡社交平台合作遏制詐騙源頭

針對網絡“刷單”或其他網絡招工詐騙的情況，可與相關社交平台建立合作，譬如中國內地警方與騰訊、阿里巴巴、美團等網絡平台已建立良好合作機制。於 2019 年 7 月 9 日，工業和信息化部網絡安全管理局會同公安部刑事偵查局、中央網信辦網絡綜合協調管理和執法督查局組織阿里巴巴、騰訊、百度、京東、字節跳動、拼多多、新浪微博、58 同城、美團、世紀佳緣、網宿科技等 11 家單位，簽訂“重點互聯網企業防範治理電訊網絡詐騙責任書”，明確必須共同維護網絡安全，建立完善詐騙風險巡查預警和快速回應處置機制，積極防範詐騙風險，對各地警方與網絡社交平台合作方面有良好示範作用。

透過與各網絡社交平台的合作，進一步加強舉報案件受理和協同聯動機制。建立完善電訊網絡詐騙舉報通報處置流程，對警察機關通報、用戶舉報的詐騙問題依法核查處置，及時回饋結果。將網絡社交平台監測發現的犯罪線索及時向警察機關通報，進一步加強訊息共享和工作聯動，形成治理合力。

此外，從中運用大數據、人工智能，對“刷單”、“招工”、“高薪”等字眼採取預警措施，對高頻發佈的詐騙帖文適時進行屏蔽及追溯消息來源，充份發揮智慧警務、主動警務的精神，繼而通過各地警務部門之間的合作機制，共享詐騙情報，共同打擊詐騙犯罪。

六、結語

現今每個國家或地區不再是一個孤立封閉的個體，勞動力的輸入和輸出已成為每個經濟體發展佈局的其中一個重要組成部分，尤其海峽兩岸及港澳人民的互動已成為常態，維護勞務人員的財產安全，避免不法分子利用求職人士渴求工作的心理而作出侵財犯罪，各地警方均責無旁貸。綜上所述，澳門警方應善用現有警務合作基礎，結合各方警務優勢，透過多邊合作，打擊和壓縮相關犯罪勢頭，避免勞務人員成為不法分子的侵害目標。

新質公安戰鬥力賦能公共安全治理：發展邏輯、理論邏輯與實踐路徑

劉蔚 *

摘要：新質公安戰鬥力是適應數智化時代發展要求，以科技創新為驅動的公安戰鬥力的再成長、再創造與再發明。新質公安戰鬥力賦能公共安全治理要堅持以人民為中心的治理價值理念、以打造全方位立體化安全網為治理變革導向、以跨中心的多元主體協同創新治理模式、以全鏈條全過程的智慧治理革新治理工具、以韌性治理提升治理效能的理論邏輯，應對國內外環境變化、非傳統領域問題凸顯、治理需求疊加、技術異化以及發展失衡等現實挑戰。探索新質公安戰鬥力賦能公共安全治理的實踐路徑，要堅持從全局角度把握公共安全治理，以韌性治理推動改革創新，加強數據安全保護，提升人才隊伍素質。

關鍵詞：新質公安戰鬥力　公共安全治理　理論邏輯　現實挑戰　實踐路徑

Empowering Public Security Governance with New Quality Public Security Combat Effectiveness: Development Logic, Theoretical Logic, and Practical Approach

Liu Wei

Abstract: The new quality of public security combat effectiveness is a response to the demands of the digital intelligence era, driven by technological innovation, fostering its growth, re-creation and reinvention. Empowering the new quality of public security combat effectiveness in public security governance requires adherence to governance values centered on the people, the direction of governance reform towards building a comprehensive, three-dimensional security network, a collaborative innovation governance model involving multiple centers, the adoption of smart governance tools across the entire chain and process, and the theoretical logic of resilient governance to enhance governance efficiency. This approach addresses real challenges such as changing domestic and international environments, the emergence of non-traditional issues, compounded governance demands, technological alienation, and imbalanced development. Exploring the practical approach to empower the new quality of public security combat effectiveness in public security governance necessitates a holistic understanding of public security governance, promoting reform and innovation through resilient governance, bolstering data security protection, and elevating the quality of talented teams.

Keywords: New Quality of Public Security Combat Effectiveness; Public Security Governance; Theoretical Logic; Real Challenges; Practical Approach

* 劉蔚，中國人民公安大學國家安全學院副教授。

一、引言

“新質公安戰鬥力”是 2024 年 1 月在全國公安廳局長會議上首次提出的重要概念，會議強調，要“高水平、保安全、促發展、推改革、抓隊伍，加快形成和提升新質公安戰鬥力，忠實履行神聖職責，奮力推進公安工作現代化，為扎實穩健推進中國式現代化貢獻公安力量。”[1] 新質公安戰鬥力意味着公安戰鬥力要實現質的變化和躍遷，它是一個動態發展性質的概念，是推動公安工作現代化、支撐高水平安全的內在要求和重要着力點。公安機關作為維護公共安全的主力軍，肩負着維護社會穩定、保障人民群眾生命財產安全的重要使命職責。當前，公共安全面對的風險挑戰日益增多，不確定性、不穩定性風險明顯增加，從反恐防暴到打擊犯罪、從社會治安到應急救援、從電信詐騙到網絡安全等，每一個環節都需要公安機關快速反應和高效應對。由此，研究新質公安戰鬥力對公共安全治理賦能的基本理論機制和實踐路徑，具有重要的理論和現實意義。

二、新質公安戰鬥力賦能公共安全治理的發展邏輯

（一）新質公安戰鬥力的基本概念與主要特徵

加快形成和提升新質公安戰鬥力，是在中國式現代化指引下，推進公安工作現代化重要支撐保障，也是以高水平安全保障高質量發展的重要基石。新質公安戰鬥力是適應數智化時代發展要求，以科技創新為驅動的公安戰鬥力的再成長、再創造與再發明。對新質公安戰鬥力的理解要從“新”與“質”兩個維度來理解，所謂“新”主要強調形勢任務之新、構建理念之新以及核心要素之新，關鍵在基於技術創新驅動的公安隊伍和公安技術發生“質”的變革。新質公安戰鬥力是指公安機關為適應新時代公安工作面對的新形勢、新問題與新任務，以公安工作現代化為追求目標，以科技創新為內在驅動力，推動公安隊伍素質、公安工作技能、公安管理和公安科技等關鍵要素的全面躍升，是推進實現具有中國特色現代警務運行體系和公安工作現代化能力的戰鬥力。新質公安戰鬥力的形成是一個動態的、積極有為的、充滿生機活力的過程，是公安機關戰鬥力不斷發展進步中實現質態躍遷變化的過程。

當前，世界未有之大變局與中華民族偉大復興的戰略全局 [2] 是公安機關新質戰鬥力首要面對的動態性全局和戰略問題。立足這一背景，構建現代警務運行體系，推進公安工作現代化，新質公安戰鬥力具有以下基本特徵：第一，在構建理念上，要堅持總體國家安全觀，不斷增強憂患意識、堅持底線思維和極限思維，隨時準備應對複雜困難的局面，有效處理各類國家安全和社會穩定問題，支撐高水平安全、保障高質量發展，滿足人民群眾的獲得感、幸福感和安全感；第二，在公安隊伍素質上，高素質的公安隊伍是加快和提升公安戰鬥力最本質要求，也是最重要的決定性要素，沒有高素質的公安隊伍就沒有高水平的新質公 安戰鬥力；第三，在公安工作技能上，新質公安戰鬥力更加要求工作技能的專業化、實戰化、法治化和科技化，不斷提升公安工作的政治能力、法律政策運用能力、防控風險能力、群眾工作能力、科技應用能力、輿論引導能力等各項技能；第四，在公安管理上，作為新質公安戰鬥力的“黏合劑”，要加快構建職能科學、事權清晰、指揮順暢、運行高效的警務管理體制；第五，在科技創新上，要充分利用大數據、物聯網、人工智慧、區塊鏈等前沿領域科技創新技術，不斷增強新質公安戰鬥力的科技創新含量，特別是關鍵核心技術的科技創新攻關，推動公安工作實現系統性的效能變革與模式重構。

（二）公安機關公共安全治理的發展與特點

公共安全是國家安全的重要組成。2022 年，黨的二十大報告在“國家安全”專章裏明確指出，要“提高公共安全治理水平。堅持安全第一、預防為主，建立大安全大應急框架，完善公共安全體系，推動公共安

[1] 中華人民共和國公安部：〈全國公安廳局長會議召開忠實履行神聖職責為扎實穩健推進中國式現代化貢獻公安力量〉，中華人民共和國公安部網站，https://www.mps.gov.cn/n2253534/n2253535/c9393980/content.html，到訪日期：2024 年 3 月 15 日。

[2] 陳建奇、高祖貴：〈新時代統籌“兩個大局”重要論述的理論意義與實踐價值〉，《學習時報》，2022 年 10 月 3 日，第 2 版。

全治理模式向事前預防轉型。”[3]2024 年，全國公安廳局長會議也特別強調，要“高品質維護公共安全”。[4]公安機關作為公共安全治理的主力軍，自新中國成立以來始終肩負着維護社會治安秩序、保障人民生命財產安全的重任，始終處於維護和塑造公共安全的第一線。

自新中國成立以降，公共安全始終是黨和政府面臨和關切的重大現實問題。建國伊始，為了鞏固新生政權，公安機關便成為應對複雜嚴峻的敵情、社情的重要力量，彼時針對特務分子、土匪惡霸、反動會道門組織、潰散武裝等反革命殘餘勢力和反動勢力進行了堅決鎮壓和取締，有效維護了社會公共安全。同時，在上海等大城市專門針對擾亂物資供應的囤積居奇等行為進行懲治，穩定市場和民心。[5] 及至改革開放和社會主義現代化建設新時期，伴隨社會變遷，流動犯罪、食品安全、公共衛生、道路交通等危害民眾生命財產安全的公共安全問題日漸凸顯，公安機關逐漸在工作思想理念、工作運行機制、行政管理模式以及隊伍建設等方面開始一系列創新改革，公眾對社會公共安全事務和公共安全事件的知情權也得到了更為有效的保障。[6] 黨的十八大以後進入新時代，我國公共安全形勢雖然總體良好，但也進入了一個公共安全事件易發、頻發和多發的時期，潛在風險和新隱患增多，防控難度加大，[7] 面對這些新挑戰和新問題，公安機關堅持總體國家安全觀，積極探索公共安全治理的新模式與新方法，融合多元主體升級立體化信息化的社會治安防控網絡，對電信詐騙、食藥環犯罪以及涉黑涉惡等突出違法犯罪精準打擊，更加注重公共安全風險預警預測預防，不斷構建智能感知的公共安全科技防控網絡，打造共建共用共治的公共安全治理體系。

在新中國 75 年的發展歷程中，因國際形勢和國內經濟社會的發展變遷，公安機關公共安全治理在不同時期有着差異化的目標任務和現實問題，但總體而言，公安機關的公共安全治理有着系統性、規範性、協調性、專業性、穩定性和創新性的變化。公安機關公共安全的治理理念從更強調安全逐漸轉變為發展和安全並重，[8] 治理模式從原有“運動式、專項化”的垂直模式向預防為主的“常態化、長效化”的扁平化模式轉變，治理主體從公安機關“單打獨鬥”的單一主體向多方參與“聯動融合”的多元主體轉變，治理手段從原有的人力為主逐漸向科技賦能轉變。

（三）新質公安戰鬥力對公共安全治理的重要意義

新質公安戰鬥力在公共安全治理中扮演着至關重要的角色。新質公安戰鬥力的底層生成根源在於科技創新驅動，科技創新發展將有效推動公安機關對公共安全治理水平的全方位提升。近年來，公安機關將大數據智能化建設作為科技興警的重要內容，積極探索智慧警務新模式，最大限度將科技發展的創新成果及時應用到公共安全治理中。如在打擊跨境電信詐騙工作中，2023 年 1 至 11 月，國家反詐中心累計下發資金預警指令 940.6 萬條，公安機關累計見面勸阻 1,389 萬人次，會同相關部門攔截詐騙電話 27.5 億次、短信 22.8 億條，處置涉詐功能變數名稱網址 836.4 萬個，緊急攔截涉案資金 3288 億。[9] 在“互聯網 + 公安政務服務”實踐中，截至 2022 年 7 月 31 日，各級公安機關依託全國公安一體化政務服務平台，上線各類網辦政務服務事項累計 3.2 萬餘項，其中 1.1 萬餘項可全程網辦。[10] 同時，在公共安全行業標準建設方面，於 2023 年，公安部就發佈安防產品、公安視頻圖像技術和移動警務技術等領域 160 項公共安全行業標準，[11] 這一系列的公共安全創新科技和標準應用，實現了社會公共安全治理效能大幅提升。

在公安機關開展公共安全治理的歷史發展進程中，科技創新驅動始終貫穿於我國革命、建設和改革發

[3] 習近平：〈高舉中國特色社會主義偉大旗幟為全面建設社會主義現代化國家而團結奮鬥〉，《人民日報》，2022 年 10 月 26 日，第 4 版。

[4] 同註 1。

[5] 王灼：〈我國公共安全治理體系的發展與完善〉，《人民論壇》，2022 年，第 5 期，第 61–63 頁。

[6] 同註 5。

[7] 范維澄：〈健全公共安全體系 構建安全保障型社會〉，《人民日報》，2016 年 4 月 18 日，第 9 版。

[8] 劉蔚：〈新安全格局的基本意涵、歷史邏輯與實踐路徑研究〉，《社會主義研究》，2024 年第 1 期，第 148–155 頁。

[9] 中華人民共和國公安部：〈公安機關打擊治理電信網絡詐騙犯罪成效顯著〉，中華人民共和國公安部網站，https://www.mps.gov.cn/n2253534/n2253535/c9367497/content.html，到訪日期：2024 年 3 月 16 日。

[10] 中華人民共和國公安部：〈推動“互聯網 + 公安政務服務”提檔升級〉，《人民公安報》，2022 年 8 月 20 日，第 1 版。

[11] 彭景暉：〈公安部：科技創新助力公安工作高質量發展〉，《光明日報》，2024 年 1 月 17 日，第 4 版。

展的各階段，不斷適應公共安全治理體系與治理能力現代化要求，維護社會安定有序。在新中國建設初期，囿於薄弱的科技基礎，公安機關在 1960 年才建立了第一家科學技術研究所。[12] 改革開放後，公安科技創新開始跨越式發展，公安機關在公共安全治理中實現了通信手段從單一到多元、電腦網絡實現突破、公共安全視頻監控快速增長、信息化應用水平顯著提高，特別是 2003 年“金盾工程”的啟動，實現了全警採集、全警應用、全警共用的公安信息化應用格局，公共安全治理精準度大幅提升。黨的十八大以後，公共安全治理的科技創新快速發展，公安機關將大數據、雲計算、人工智慧、移動互聯網、物聯網等技術與公安各業務領域深度融合，自 2016 年開始推動綜合性平台建設，推進合成作戰、視頻圖像聯網、警務綜合、移動警務，公安機關實現了信息的全面彙聚和深度挖掘，有效提高了對公共安全風險的預測預防和打擊處置能力，推動公共安全治理更加智能化、精準化，實現了多警種、多部門的協同治理效能，推動了公安機關公共安全治理體系和治理能力的現代化。

三、新質公安戰鬥力賦能公共安全治理的理論邏輯

（一）治理價值理念：堅持以人民為中心

加快和提升新質公安戰鬥力是在聚焦經濟建設這一中心工作和高質量發展這一首要任務 [13] 的大背景下提出的，這就意味公安機關在公共安全治理中要以高水平安全保障高質量發展。在實踐發展中，高質量發展與高水平安全在根本上還是解決人民群眾的安全需求，在任何時候人民的生命財產安全都是第一位的，以人民為中心的價值理念是黨和政府工作的根本出發點和落腳點。以科技創新驅動的新質公安戰鬥力，就是借助科技力量更加精準高效地提升警務工作智能化水平、精準打擊和高效防範公共安全風險威脅、為人民群眾提供優質高效的公共安全服務產品，為公共安全這一基本社會民生問題提供了全方位、多層次的科技保障。與此同時，新質公安戰鬥力賦能公共安全治理的成效如何，也是要由人民來評判，以人民安全感和滿意度為檢驗標準。只有保障人民生命財產安全，堅持一切為了人民、一切依靠人民，才能真正實現人民的幸福感、獲得感和安全感，滿足人民群眾對美好生活的嚮往和追求。

（二）治理變革導向：打造全方位立體化安全網

公共安全治理是一個多元化、多領域、多時空交織的複雜系統，牽涉面廣，涉及領域多，時空交織疊加的複合屬性強。新質公安戰鬥力推動公共安全治理就是要實現科技與治理的深度有機融合，突破原有單一層面、單一部門、單一領域、單一時空以及單一問題的邊界限制，構建要素之間、領域之間的縱橫互聯以及虛擬空間和現實空間的同頻共治複雜網絡。一是要實現公共安全治理的現代科技融合，能夠有效借助大數據、雲計算、物聯網、區塊鏈、移動互聯網以及人工智慧等現代科學技術，實現技術之間的良性互動，形成高效有序、預警預測以及智能決策的公共安全治理平台；二是要實現公共安全治理的三重空間融合，通過現代科技形成物理空間、信息空間以及心理空間的有效信息整合，實現公共安全治理問題和風險的“神經末梢”智能感知，從技防、人防和物防等方面，形成對規律性事件和突發性事件的針對性和實效性處置。由此，基於現代科技融合的治理平台，實現物理空間、信息空間以及心理空間的有效整合，打造公共安全治理全方位立體化安全網。

（三）治理模式創新：跨中心的多元主體協同

當前，傳統公共安全的“一元治理”模式，即以政府為唯一主體的治理方式，已經難以適應現代社會的多元化和複雜性。新質公安戰鬥力賦能公共安全治理，意味着通過科技驅動實現多元主體的跨中心協同治理模式，這一模式突破了原有政府主體單一治理以及企業、社會組織、基層社區和普通民眾等各主體獨立治理的困境。在傳統的多元主體協同治理模式中，雖然也強調多元主體的參與，但往往缺乏系統聯動和整

[12] 鶴崗網警：〈回眸輝映科技之光 激發跨越發展新動能〉，百度百家號網站，https://baijiahao.baidu.com/s?id=1644252436760581077，到訪日期：2024 年 3 月 16 日。

[13] 人民日報：〈中央經濟工作會議在北京舉行〉，《人民日報》，2023 年 12 月 13 日，第 1 版。.

體協同的跨中心機制。而在新質公安戰鬥力賦能下，跨中心的多元主體協同模式將每一個公共安全治理要素主體視為一個中心，在即時監測公共安全事件或預測公共安全風險的全方位立體化公共安全網前端感知下，一旦預測到風險威脅，每個要素主體均能夠迅速反應，進行系統聯動、整體協同、力量整合。這種高效協同的方式，能夠最大限度地實現要素主體形成的關係網絡的良性互動，提高公共安全治理的效率和效果。同時，跨中心的多元主體協同也意味着打破信息孤島，提高公共安全治理的透明度和公信力。

（四）治理工具革新：全鏈條全過程的智慧治理

伴隨現代社會運行體系的日益複雜與安全風險的不斷增加，公共安全治理已然向風險預防、風險治理、協同應對以及韌性提升的可持續發展轉變。新質公安戰鬥力賦能公共安全治理要從感知鏈、評估鏈、預案鏈、決策鏈、處置鏈等治理全鏈條的工具革新實現精細化治理。治理工具革新並非是廣義角度政策、方案和技術的治理工具，而特指狹義角度的技術層面治理工具革新。在感知鏈，主要是基於物聯網泛在接入技術，即時採集公共安全治理社會面上“神經末梢”的物聯網感知數據，形成數據池；在評估鏈，主要是通過對結構化數據、半結構化數據和非結構化數據的大數據挖掘，並借助知識圖譜、機器學習和深度學習等人工智慧技術輔助分析，形成事件評估鏈條；在預案鏈，通過三維可視化仿真推演模擬技術，對公共安全治理對象、環境和事件進行三維真實再現，形成預案模擬；在決策鏈，通過預案模擬結合 5G、人工智慧分析、無人機以及北斗衛星定位等技術，借助輔助決策知識模型，提出公共安全治理決策科學依據，提高決策準確性和時效性；在處置鏈，通過跨中心的多元主體協同機制平台，結合智能化資源保障與應用平台，通過全警應用的警務移動終端，形成人力調配、資源協調、事件處置、高效監管、全程評估相銜接的數智處置鏈。由此，充分發揮新質公安戰鬥力賦能公共安全治理的“數據 +AI+ 決策 + 協同 + 體系”全鏈條全過程的智慧治理聚合效應，因勢、因時、因地、因事、因人智慧化統籌實現公共安全精細化治理。

（五）治理效能提升：推動公共安全韌性治理

2015 年聯合國可持續發展峰會通過的《改變我們的世界：2030 年可持續發展議程》將建設包容、安全、有抵禦災害能力和可持續的城市和人類住區作為 2030 年可持續發展目標之一。[14] 新質公安戰鬥力賦能公共安全治理，是全方位、多層次、高效率的賦能，其治理效能提升的關鍵體現在公共安全事件與風險治理中抵禦、適應以及吸收風險的效能以及恢復效能。在大數據、雲計算、人工智慧、物聯網等一系列的現代科技驅動賦能之下，公安機關通過打造全方位立體化安全網、跨中心的多元主體協同以及全鏈條全過程的精細化治理，真正實現技術融合、空間融合、主體融合、平台融合、資源融合等多方面的融合創新，提升跨層級、跨地域、跨系統、跨部門、跨業務的系統協同，從“前端感知—事件評估—預案模擬—智慧決策—數智處置”這一全鏈條上形成治理聚合效應，全方面增強公安機關公共安全治理的領導力、規劃力、執行力、控制力、評估力、適應力、恢復力等多維能力，[15] 從而真正實現公安機關公共安全治理效率與效能的顯著提升，不斷夯實公安機關公共安全治理的各方面全過程基礎。

理論基礎	驅動要素	關鍵內容
治理價值	堅持以人民為中心	人民至上，一切為了人民、一切依靠人民
治理變革	全方位立體化安全網	實現公共安全治理的現代科技融合，三重空間融合
治理模式	跨中心的多元主體協同	跨中心的多元要素主體關係網絡的良性互動，破除信息孤島，提高公共安全治理的透明度和公信力

[14] 王婷：〈韌性社會治理：社會系統安全穩定運行的實踐進路〉，《光明日報》，2020 年 6 月 12 日，第 11 版。

[15] 靳諾：〈把我國制度優勢更好轉化為國家治理效能〉，《光明日報》，2021 年 1 月 13 日，第 9 版。

理論基礎	驅動要素	關鍵內容
治理工具	全鏈條全過程的智慧治理	感知鏈、評估鏈、預案鏈、決策鏈、處置鏈等治理全鏈條的工具革新，“數據 +AI+ 決策 + 協同 + 體系”的全鏈條全過程智慧治理聚合
治理效能	韌性治理	增強公安機關公共安全治理的領導力、規劃力、執行力、控制力、評估力、適應力、恢復力

表1　新質公安戰鬥力賦能公共安全治理的理論基礎

四、新質公安戰鬥力賦能公共安全治理面對的現實問題

（一）公共安全治理面對的內外環境：不確定性不穩定性增強

當今世界，百年未有之大變局加速演進，世界進入新的動盪變革期，國際秩序處於新舊轉換期，國際力量對比持續變化，地緣戰略格局深度調整，大國關係持續變化，新一輪科技革命和產業變革給全球安全治理帶來了全新挑戰，國際形勢日趨錯綜複雜，不確定性、不穩定性、超預期性因素顯著增多。在傳統不安全因素仍未消除的境況下，全球性的非傳統安全威脅持續蔓延，跨國安全威脅、生態環境威脅、疾病傳染病等全球公共安全衛生威脅、恐怖主義威脅構成了新的全球不安全因素的重要來源。[16] 面對國際形勢的時局、勢局與局部亂局，在市場經濟轉軌和社會結構轉型的發展變遷中，我國發展仍存在諸多深層次、周期性和結構性、體制性問題，依然需要面對自身發展的不平衡不充分問題，地區差距、城鄉差距、收入差距等問題依然存在，在教育、醫療、住房、養老等方面還有不少問題需要解決，不同類型的社會矛盾交織疊加，公共安全治理的挑戰風險日漸增多，各種“黑天鵝”、“灰犀牛”事件隨時可能發生。

（二）公共安全治理面對的風險趨勢：非傳統領域安全風險顯著上升

伴隨着時代的持續進步與全球化的深入發展，公安機關在公共安全治理領域所面臨的國內外環境日趨複雜且多變。在追求高質量發展與高效能治理的征途上，公安機關正遭遇着各類非傳統安全風險的急劇增長，這些風險以指數級態勢擴張，導致公共安全事件愈發頻繁且多樣化。尤其值得關注的是，經濟安全、金融穩定、科技創新安全、能源保障、生態環境保護、社會安定、糧食自給自足以及生物安全等非傳統安全領域的問題正日益凸顯。這些問題呈現出跨區域的擴散、跨領域的交融、跨時空的疊加，以及相互之間的聯動性增強和源頭多元化等現實性的特徵。在致災因素複合疊加、孕災環境複雜多變、風險事件關聯互動性增強的態勢下，[17] 非傳統領域的安全風險對公共安全治理構成了重大挑戰。特別是在超大城市和大城市中，其空間人口壓力進一步加劇了非傳統領域安全的複雜性，一系列的城市病與突出違法犯罪、社會治安問題、公共交通安全、疾病流行等公共安全治理難題交織疊加，導致治理難度進一步加大，極易形成公共安全治理風險綜合體。

（三）公共安全治理面對的治理需求：多層次多元化相疊加

面對不確定不穩定的內外環境以及非傳統領域安全風險的日益凸顯，公安機關公共安全治理需要應對多層次、多元化的治理需求挑戰。就我國現實而言，多層次的公共安全治理需求從廣義層面來說主要包括不同層面、不同領域和不同功能的治理。[18] 其中，不同層面的公共安全治理需求涵蓋了我國東部、中部、西部以及城市和鄉村等不同地區的差異化需求，也涉及國家、社會和個人等不同層次的治理需求；不同領域主要強調了應對傳統公共安全領域和非傳統公共安全領域、虛擬空間領域和現實空間領域以及虛實交織領域的

[16]　肖歡容、張沙沙：〈全球安全治理的緣起及挑戰〉，《江西社會科學》，2018 年，第 11 期，第 209–217 頁。

[17]　韓廣華：〈全面提高公共安全保障能力 牢牢守住安全發展底線〉，中華人民共和國應急管理部網站，https://www.mem.gov.cn/xw/ztzl/2020/xxgcwzqh/qwjd/zjjd/202012/t20201208_374878.shtml，到訪日期：2024 年 3 月 17 日。

[18]　翁士洪、周一帆：〈多層次治理中的中國國家治理理論〉，《甘肅行政學院學報》，2017 年，第 6 期，第 4–14 頁、第 125 頁。

公共安全治理需求；不同功能主要強調了不同層面和不同領域的政策、方案和技術工具對公共安全治理的需求。而多元化主要指涉及政府、企業、社會組織、基層社區以及普通民眾等多元主體對公安機關公共安全治理的需求。值得注意的是，在推進中國式現代化進程中，多層次以及多元化的公共安全治理需求並非是確保不發生公共安全事件的基礎性需求，而是要適應數智化時代、內外環境變化以及非傳統安全領域問題的預防在先、化解在先、服務在先的高品質安全需求。

（四）公共安全治理面對的技術風險：技術賦能的多維異化

以科技創新驅動的新質公安戰鬥力對公共安全治理的賦能主要強調數字智能技術的全面應用，但如果技術應用無邊界、無規則或是無制約將給公安機關的公共安全治理帶來“異化”風險，要警惕“數字失能”、“數字官僚”、“數字侵害”、“數據洩露”等多維技術異化問題。在數字失能方面，基於大數據、雲計算、物聯網、人工智慧等技術構建起的技術平台，往往忽視社會要素的多變性和複雜性，單純的數據治理可能會產生“數據偏誤”和“決策偏差”，同時也會對諸如老年群體等對現代科技難以適應的群體構成“數字歧視”；在數字官僚方面，單純的數字技術依賴可能會使公安民警成為數字技術的附庸，削弱公安民警對治理對象的人文關懷，也會使基層公安民警產生一定的技術運用心理壓力；在數字侵害方面，公安機關如果沒健全的制度建設或是演算法平衡，容易導致部門利益或個人權力凌駕於技術使用的合理範疇，進而使得數字技術在公共安全治理應用中侵蝕民眾合法權利；在數據洩露方面，公安機關確保政府數據、社會數據、個人數據以及技術數據的使用安全性和合法性，避免數據洩露，保護民眾個人隱私。

（五）公共安全治理面對的發展失衡：技術推進的滯後風險

當前，我國發展不平衡不充分的問題仍然突出，公安機關公共安全治理也需要面對發展過程中地區失衡、制度失衡、群體失衡、認知失衡等多種問題，這也事實上反映了新質公安戰鬥力賦能公共安全治理的螺旋式發展過程。從地區失衡來看，因經濟社會發展的地域差異性，極易導致公共安全治理數智化轉型的地區差異性，各地公安機關機制建設平台系統搭建主體協同等方面均會呈現建設的階梯差異性；從制度失衡來講，主要防範技術賦能過程中硬體建設超前於法律制度機制政策方案的建設而導致的制度性滯後，進而導致缺乏約束的技術建設；從群體失衡上看，主要強調差異化群體對於公共安全治理技術的使用失衡，以及不同群體對公共安全治理技術接受意願的差異性，進而導致群體不滿或激憤；在認知失衡方面，主要是指公安機關在推進公共安全治理技術過程中不同層級領導和公安民警對於技術創新驅動的認知上的差異，從而導致頂層設計的偏誤、制約數據跨部門整合使用，嚴重的甚至會將公共安全治理視為新的“面子工程”。

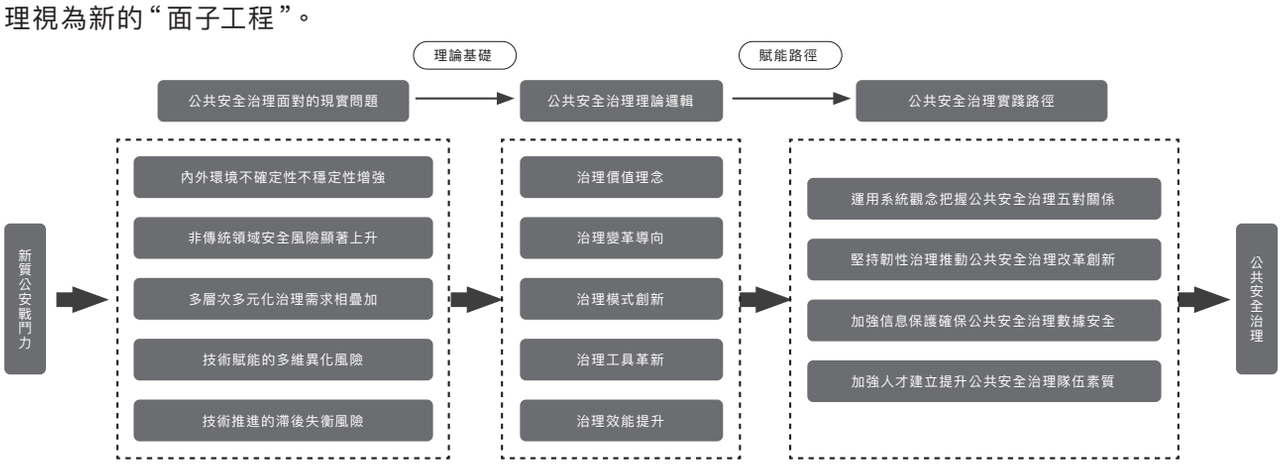

圖1　新質公安戰鬥力賦能公共安全治理框架圖

五、新質公安戰鬥力賦能公共安全治理的實踐路徑

（一）運用系統觀念，把握公共安全治理五對關係

新質公安戰鬥力賦能公共安全治理是一個系統工程，要從全局的角度運用系統觀念推進公安機關公共安全治理，遵循整體性、結構性、層次性、開放性的思維方式，加強前瞻思考、全局謀劃、戰略佈局和整體推進，不能各管一攤、相互掣肘，必須統籌兼顧、整體施策、多措並舉，堅持底線思維和極限思維，全方位、全領域、全過程地推進新質公安戰鬥力賦能公共安全治理。在運用系統觀念的思維方式上，要統籌把握好五對關係，一是新質公安戰鬥力賦能公共安全治理與國內外大環境之間的關係；二是公安機關公共安全治理整體性與新質公安戰鬥力構成要素之間的關係；三是公安機關公共安全治理基礎要素與關鍵要素之間的結構性關係，四是新質公安戰鬥力賦能公共安全治理中跨中心的多元主體協同關係；五是新質公安戰鬥力賦能公共安全治理運行規律與優化提升之間的關係。同時，以前瞻性思考把握分析公共安全治理數智化轉型的挑戰機遇，以全局意識將新質公安戰鬥力放到公共安全治理工作大局中思考定位，以戰略眼光和戰略智慧推動新質公安戰鬥力為公共安全治理帶來戰略突破，以整體推進增強公安機關公共安全治理的系統平衡與重點突出。特別注意的是，新質公安戰鬥力賦能公共安全治理，不能忽視可預料和難預料的風險挑戰，要堅持底線思維和極限思維，強化憂患意識、危機意識，要做好未雨綢繆、防微杜漸，從極端風險挑戰的“上限”與不能突破的“下限”考慮好、設定好，更精準、更科學、更主動地應對風險挑戰，注重風險挑戰的整體性、關聯性，保障全局性新質公安戰鬥力賦能公共安全治理的耦合性。

（二）堅持韌性治理，推進公共安全治理改革創新

韌性治理是以彈性調適為目標的公安機關新型公共安全治理理念，在系統觀念的指引下，公安機關的公共安全韌性治理要不斷提升改革創新意識和思維能力，在公安機關公共安全治理的“求變”與“求異”中不斷完善韌性治理制度，健全全鏈條的韌性治理機制。具體而言，一是在“求變”過程中，要準確識別新質公安戰鬥力賦能公共安全治理的新變化、主動立足現代科技融合與創新謀求公安機關公共安全治理迭代升級，從公共安全治理對象、治理科技、各級治理運行機制模式、治理整體防控、治理執法監督管理、治理專業化實戰化職業化隊伍建設等全方面實現科技賦能創新；二是在“求異”過程中，要結合公安機關公共安全治理的地區差異、群體差異、需求差異、認知差異、制度差異等異質性特徵，借助科技創新驅動的新質公安戰鬥力利用“數智科技”的現代科技組合彌補公安機關公共安全治理的異質的鴻溝，完善“ 專業 + 機制 + 大數據”的新型警務運行模式；三是在“求變”與“求異”中，要及時推進韌性制度建設，包括彌補公共安全治理領域的立法空白點、完善新質公安戰鬥力賦能公共安全治理的內部制度建設、培育新質公安戰鬥力賦能公共安全治理的文化建設；四是針對偶發性公共安全事件和規律性公共安全事件，從公安機關公共安全治理的感知鏈、評估鏈、預案鏈、決策鏈、處置鏈等方面，全鏈條關注公共安全事件發展，重視物理環境和情境的恢復，也重視跨中心多元主體的心理情境恢復，[19] 從而滿足多層次多元化的治理需求。

（三）加強信息保護，確保公共安全治理數據安全

數據是新質公安戰鬥力賦能公共安全治理的關鍵資源，也制約着大數據、雲計算、人工智慧等新興科技應用於數字智慧治理的廣度和深度，要特別注重從公共安全治理的制度建設和現實應用等維度確保數據安全。一是在新質公安戰鬥力賦能公共安全治理平台方面，要加強智能決策的監督、審查和控制，避免決策過程中“演算法決策”對民眾正當權益的侵害，也確保數智決策本身的程式合法性、內容合法性；二是要加強數據安全監測，明確公安機關數智公共安全治理過程中數據使用以及具體執法過程中的義務和責任，特別是避免對本源數據和系統使用痕跡的非法篡改、抹除，防止數據密案失洩事件發生；三是要強化公安機關公共安全治理中的數據技術安全，不斷加強基礎軟體技術和關鍵信息基礎設施等方面的自主創新，既要在晶片、數據存儲介質等系統硬體和操作系統、資料庫、大數據軟體、分析工具等軟體上確保安全可信，

[19] 易承志：〈中國韌性治理體系的框架和構建路徑〉，《人民論壇》，2023 年，第 15 期，第 66–69 頁。

也要確保數據採集、傳輸、存儲、處理、交換和銷毀等各階段的安全審計以及其他技術應用上的數據資產安全；四是在公共安全治理數據安全制度建設方面，要隨時根據科技賦能現實發展優化法律法規制度、組織保障制度、監管執行制度、數據安全評價制度，對數據安全形成全生命週期的制度保障。

（四）加強人才建設，提升公共安全治理隊伍素質

人才隊伍是公安工作現代化的生力軍，也是新質公安戰鬥力賦能公共安全治理的核心助推器。在科技創新驅動的公共安全治理中，要堅持做好公安隊伍人才培育。一是要加強公安隊伍思維認知理念，既要充分意識到數智時代公共安全治理數智化轉型的發展大趨勢，及時轉變工作思維和對科技賦能的認知，也要打破“跟跑”觀念和破除“論資排輩”的思想觀念束縛，各級領導幹部要具備創新思維和創新意識；二是要提升公安隊伍人才引進的精準度和適配度，嘗試實行公共安全治理緊缺人才清單制度，完善公安隊伍公共安全治理人才培養、引進、使用與合理流動的工作機制，推動人才這一“關鍵變數”成為新質公安戰鬥力賦能公共安全治理的“最大增量”；三是要着力培養公安機關政治素質可靠、技術能力過硬的高素質創新拔尖人才，破除地區和治理領域人才異質性所導致的治理失衡，走好公安院校人才培養之路和高等院校人才輸送之路，前瞻性制定和實施公共安全治理創新拔尖人才戰略規劃，整合各級公安機關、公安科研機構、公安院校和普通高校與研究機構之間科研資源、教育資源、行業資源和社會資源，做好公安機關人才培養協作的人才鏈，充分啟動人才培養流動的各環節，堅定走好高素質公安隊伍人才的自主培養之路，讓更多高素質人才成為新質公安戰鬥力賦能公共安全治理的引領者、踐行者和見證者。

六、結語

當前，世界百年未有之大變局加速演進，國內外環境的不穩定性不確定性增強，公共安全治理面對諸多現實性挑戰。新質公安戰鬥力賦能公共安全治理關鍵在於科技創新驅動的公安隊伍和公安技術發生“質”的變革，要堅持以人民為中心的治理價值理念，將打造全方位立體化安全網作為治理變革的導向，實現治理模式的跨中心多元主體協同創新體系，推動全鏈條全過程的智慧治理工具革新，推動公共安全韌性治理的效能提升。然而，在現實實踐中仍然需要面對內外環境變化、風險挑戰增加、多層次多元化治理需求疊加、技術賦能的異化風險以及技術推進中的發展失衡等方面的關鍵問題和衍生性問題。有鑑於此，要具備戰略眼光和系統思維，將新質公安戰鬥力賦能公共安全治理視為一個系統工程，積極、有效、務實地推進公共安全治理改革創新，確保公共安全治理數據安全，提升公共安全治理隊伍素質。

基於人工智慧的新型犯罪對公共安全的威脅及其應對措施

雲暉欽 *

摘要：本論文旨在探討基於人工智慧的新型犯罪手法，並提出相應的應對策略。通過對法律和政策層面、技術層面以及教育和意識層面的分析和討論，本文總結了應對基於人工智慧的新型犯罪的關鍵策略。在法律和政策層面，制定和完善相關法律法規、加強國際合作和提高公眾意識是關鍵。在技術層面，創新網絡安全技術和人工智慧演算法對於預防和應對犯罪，具有重要作用。在教育和意識層面，提高公眾的數字素養和網絡安全意識是至關重要的。然而，應對基於人工智慧的新型犯罪仍面臨挑戰，需要進一步完善法律框架、推動技術創新、加強教育和意識提高，並加強國際合作。

關鍵詞：新型犯罪　法律和政策　技術創新　教育和意識　國際合作

Threats of Emerging AI-Based Crimes to Public Safety and Countermeasures

Wan Fai Iam

Abstract: This paper aims to explore the emerging AI-based crime trends and propose corresponding strategies to address them. Through the analysis and discussion from the legal and policy aspects, technological aspects, and education and awareness aspects, this paper summarizes the key strategies to combat AI-based crimes. At the legal and policy level, the key lies in formulating and improving relevant laws and regulations, strengthening international cooperation, and raising public awareness. At the technological level, innovation in cybersecurity technologies and AI algorithms play a crucial role in crime prevention and response. At the education and awareness level, enhancing public digital literacy and cybersecurity awareness is of paramount importance. However, there are still challenges in addressing AI-based crimes, thus requiring further optimization of legal frameworks, promotion of technological innovation, strengthening of education and awareness, and the intensification of international cooperation.

Keywords: Emerging AI-Based Crimes; Legal and Policy; Technological Innovation; Education and Awareness; International Cooperation

* 雲暉欽，澳門保安部隊高等學校第十八屆消防官培訓課程學員。

一、前言

近年來，隨着人工智慧（AI）技術的飛速發展，社會正在經歷着前所未有的變革。AI 技術已經逐漸滲透到各個領域，為我們的生活帶來了諸多便利和創新。然而，隨着 AI 技術的廣泛應用，我們也面臨着新形式的犯罪威脅。據《全球犯罪報告 2022》的數據顯示，基於 AI 的新型犯罪呈現出快速增長的趨勢，犯罪分子利用 AI 技術來規劃和實施犯罪行為，使其更加隱蔽和複雜。網絡犯罪、金融欺詐、數據洩露等領域已成為他們活動的主要目標。[1] 這些新型犯罪活動主要涉及利用機器學習、數據挖掘和圖像識別等技術。通過這些技術，犯罪分子能夠更加隱蔽地操縱和實施犯罪行為，使傳統的執法手段變得不再有效。

為了更好地理解基於 AI 的新型犯罪對公共安全的威脅，我們可以回顧一些實際案例。例如，在網絡犯罪領域，犯罪分子利用 AI 技術進行釣魚攻擊、勒索軟體攻擊和網絡入侵行為，導致個人和組織的財務損失及信息洩露。此外，AI 技術的發展還為虛假信息的生成和傳播提供了便利，進一步加劇了社會的混亂和不穩定。

本文旨在深入探討基於 AI 的新型犯罪對公共安全的威脅及其應對措施。通過分析實際案例和研究現狀，我們將深入了解新型犯罪的特徵和範圍，並探討其對公共安全和社會穩定的影響。同時，我們將提出有效的應對措施，包括法律和監管措施、技術解決方案、加強合作與信息共用以及提升公眾意識和教育等。通過對基於 AI 的新型犯罪威脅的研究，我們可以為公共安全和社會穩定提供更有效的保護和防範措施。只有深入了解和應對這一威脅，我們才能確保人工智慧技術的健康發展，並使其為社會帶來更多的利益和福祉。

二、基於人工智慧的新型犯罪手法的定義和分類

（一）基於人工智慧的新型犯罪的定義和特點

新型犯罪是指利用最新科技和先進技術手段進行的犯罪活動。其中，利用人工智慧技術進行的犯罪已成為新型犯罪的重要組成部分。這類犯罪形式通過運用人工智慧演算法、機器學習、自然語言處理和大數據分析等技術手段，使犯罪分子能夠更隱蔽、高效地策劃、執行和掩蓋犯罪行為。[2]

其特點主要包括：[3]

1. 自動化

人工智慧技術使犯罪分子能夠自動化地執行犯罪活動。利用機器學習和演算法分析，犯罪分子能快速、大規模地實施網絡攻擊、欺詐和信息洩露等行為，且不易被發現。

2. 智能化

人工智慧的智能化特性使犯罪分子能夠更巧妙地規劃和執行犯罪活動。通過自然語言處理和深度學習，他們能製造逼真的虛假信息、進行社交工程攻擊或操縱市場價格等，更易逃避偵查和打擊。

3. 數據驅動

人工智慧技術使犯罪分子能更有效地獲取、分析和利用大規模數據。通過數據挖掘和預測分析，他們能精準識別潛在受害者、漏洞和機會，提高犯罪的針對性和成功率。

4. 跨界性

人工智慧的跨領域應用為犯罪分子提供了更多機會和手段。新型犯罪涉及網絡、金融、身份盜竊、信息傳播等多個領域，使其更具複雜性和多樣性，且不受地域和法律限制。

---

[1] Smith, J., & Johnson, A. (2022). The Impact of Artificial Intelligence on Cybercrime. MIT Technology Review.

[2] 馬榮春：〈論新型犯罪對刑法理論的影響：以網絡犯罪為中心〉，《學術界》，2022 年，第 4 期，第 126–142 頁。

[3] 楊昌軍：〈中國社會新時代的新型犯罪治理機制——以羅師莊社群為樣本的實證研究〉，《犯罪研究》，2017 年，第 5 期。

（二）基於人工智慧的新型犯罪的種類

基於人工智慧的新型犯罪主要分為以下幾類：[4]

1. 虛假信息傳播

詐騙分子利用 AI 技術生成虛假新聞、評論和社交媒體帖子，通過操縱輿論和市場情緒誤導公眾，以獲取非法利益。這些虛假信息具有很高的迷惑性，難以分辨。

2. 仿冒身份詐騙

利用 AI 技術生成逼真的聲音和圖像，詐騙分子可以冒充他人身份進行欺詐活動。他們通過模仿他人的聲音或生成逼真的視頻圖像，騙取受害人的信任和財產。

3. 個人信息盜竊

利用 AI 技術分析和破解個人信息，詐騙分子獲取用戶的敏感信息，如銀行帳號、信用卡信息等。通過竊取個人信息，詐騙分子能夠實施各種欺詐行為，甚至直接盜取受害人的財產。

4. 金融欺詐

利用 AI 技術進行市場操縱、欺詐交易和投資詐騙，詐騙分子非法獲取巨額財富。通過分析市場數據和交易行為，詐騙分子能夠發現投資者的弱點，制定針對性的欺詐策略，導致投資者遭受重大損失。

綜上所述，以上四類是基於人工智慧的新型犯罪最常見的類型。然而，由於人工智慧具有快速迭代和自我演變的特性，可以預見，利用人工智慧的新型犯罪也將不斷迭代和更新。在未來，基於人工智慧的犯罪將催生出更多樣化、難以預測的新式犯罪。因此，打擊新型犯罪的工作仍然任重道遠。

三、基於人工智慧的新型犯罪對公共安全的威脅

（一）構成全球範圍內的公共安全威脅

隨着人工智慧（AI）技術的廣泛應用，基於 AI 的新型犯罪手法不斷湧現，對公共安全構成嚴重威脅。這些犯罪活動涉及財產損失、個人信息洩露和社會穩定性下降等方面，對個人、組織乃至整個社會造成巨大影響。

1. 財產損失

基於人工智慧的犯罪活動導致財產損失的問題日益嚴重。根據《IBM X-Force 威脅情報季度報告》，網絡犯罪活動每年給全球經濟帶來數十億美元的損失。這些損失主要源自金融欺詐、網絡釣魚攻擊和勒索軟體等犯罪行為。[5]

金融欺詐利用 AI 技術的高度精確性和自動化能力，使犯罪分子能夠更有效地進行詐騙活動。他們利用機器學習和演算法分析，針對個人和企業的財務信息進行竊取和濫用，導致巨額經濟損失。網絡釣魚攻擊則通過偽裝成合法機構或個人，誘使受害者洩露個人敏感信息或進行不正當交易，從而獲取經濟利益。勒索軟體攻擊利用 AI 技術的加密和擴散功能，對個人或組織的電腦系統進行惡意鎖定和信息加密，迫使受害者支付贖金以恢復數據或解除鎖定。

2. 個人信息洩露

基於人工智慧的新型犯罪手法還導致個人信息洩露問題日益嚴重。根據《Verizon 數據洩露調查報告》，數據洩露事件的數量和規模呈現出快速增長的態勢，導致大量個人敏感信息被非法獲取和利用。[6]

犯罪分子利用 AI 技術分析和破解個人信息，竊取用戶的敏感數據，如姓名、地址、社會安全號碼等。這些信息被用於身份盜竊、金融欺詐等非法活動，給受害者帶來嚴重的隱私和安全風險。此外，數據洩露事件還對企業和政府機構的聲譽造成負面影響，導致公眾信任度下降，進而影響整個社會的穩定性。

---

[4] 王力一：〈智能犯罪的特徵、類型及應對策略〉，《遼寧警專學報》，2005 年，第 4 期。

[5] 石晗、鄭禮平：〈新時代大學生網絡犯罪的現況與預防對策探析——基於 76 例案例的實證研究〉，《法學》，2023 年，第 11 卷，第 6 期。

[6] 吉克：〈論地方性個人資料保護法律制度之建構——以澳門特區為例〉，《區域治理》，2023 年，第 27 期，第 191–194 頁。

3. 社會穩定性下降

基於人工智慧的虛假信息傳播對社會穩定性產生了負面影響。虛假信息通過 AI 技術生成和擴散，誤導公眾輿論，引發社會混亂和信任危機。這些虛假信息可能涉及政治、經濟、社會等各個方面，旨在製造矛盾、煽動情緒或干擾正常秩序。它們往往具有高度的逼真性和隱蔽性，難以被公眾辨識和抵制。

虛假信息的傳播可能導致社會不滿情緒的加劇、社會分裂的擴大，以及國家和地區的穩定受到威脅。例如，通過操縱輿論和市場情緒，犯罪分子利用 AI 技術誤導公眾決策，導致市場波動和社會動盪。此外，虛假信息還可能干擾正常的政治進程和選舉結果，破壞民主制度的正常運行。

綜上所述，基於人工智慧的新型犯罪手法對公共安全構成嚴重威脅，涉及財產損失、個人信息洩露和社會穩定性下降等方面。為了應對這些威脅，國際社會需要加強合作，制定更加有效的法律與政策，提高技術防範能力，並加強對公眾的教育和意識提升。通過這些措施的綜合應用，我們可以更好地保障公共安全和社會的穩定發展。

（二）構成我國範圍內的公共安全威脅

隨着人工智慧（AI）技術的快速發展和廣泛應用，我國也面臨着基於 AI 的新型犯罪所帶來的公共安全威脅。這些犯罪活動不僅對公民的財產和信息安全構成嚴重威脅，還對社會穩定和法治建設造成負面影響。

1. 公民的財產受到重大威脅：基於人工智慧的欺詐活動

近年來，我國金融欺詐案件數量呈上升趨勢，給個人和企業造成了巨大的經濟損失。根據國家金融監督管理總局的統計數據，2022 年我國基於人工智慧技術的金融詐騙案件數量高達 50 萬起，涉及金額超過 100 億元。這些犯罪分子利用 AI 技術的高度精確性和自動化能力，實施各種詐騙活動，如網絡釣魚、虛假投資、偽造交易數據等。[7]

除了金融欺詐外，基於人工智慧的惡意軟體也廣泛應用於網絡釣魚攻擊和勒索行為。犯罪分子利用 AI 技術偽造電子郵件、網站等手段，誘騙受害者點擊惡意鏈接或下載病毒，進而竊取個人信息或對電腦系統進行破壞。同時，駭客利用 AI 技術自動化地破解密碼和安全防護系統，對個人和企業網絡系統進行入侵和攻擊，導致數據洩露和財產損失。

2. 公民信息洩露：基於人工智慧的數據安全威脅

隨着數位化進程的加速，個人信息在互聯網上的傳播愈發廣泛，但同時也面臨着更大的安全風險。犯罪分子利用人工智慧技術高效地分析和破解個人信息，導致大量個人敏感數據被盜取和濫用。根據《中國互聯網絡信息中心》的報告，我國個人信息洩露事件在過去幾年中呈上升趨勢，涉及姓名、身份證號碼、聯繫方式等敏感信息。[8]

個人信息洩露給個人隱私和安全帶來了嚴重威脅，同時也為企業和政府機構的運營和聲譽帶來負面影響。犯罪分子利用竊取的個人信息進行身份盜竊、金融欺詐等非法活動，給受害者帶來巨大的經濟損失。此外，這些數據還可能被用於政治目的和社會不穩定活動，對國家安全和社會穩定造成威脅。

3. 破壞社會的法治建設和誠信體系：基於人工智慧的虛假信息和輿論操縱

人工智慧技術也給虛假信息和輿論操縱提供了便利。犯罪分子利用 AI 技術生成和傳播虛假信息，誤導公眾輿論，對社會穩定產生負面影響。這些虛假信息可能涉及政治、經濟、社會等各個方面，旨在製造矛盾、煽動情緒或干擾正常秩序。它們往往具有高度的逼真性和隱蔽性，難以被公眾辨識和抵制。

犯罪分子通過社交媒體平台等渠道廣泛傳播虛假信息，利用機器人和假帳戶模仿人類行為進行評論、點讚和轉發等操作，以操縱輿論和誤導公眾。這種行為不僅破壞了信息的真實性，還可能引發社會不滿情緒的加劇、社會分裂的擴大，以及國家和地區的穩定受到威脅。同時，人工智慧技術也給網絡駭客

[7] 林平：澎拜新聞，〈公安部：破獲“AI 換臉”案 79 起，抓獲犯罪嫌疑人 515 名〉，發佈日期：2023 年 8 月 10 日，網址：https://www.thepaper.cn/newsDetail_forward_24180052，到訪日期：2024 年 1 月 20 日。

[8] 賈金月：〈APP 侵犯個人信息的實證研究〉，《爭議解決》，2023 年，第 9 卷，第 6 期。

提供了便利，使得網絡詐騙、惡意軟體、網絡攻擊等犯罪行為更加隱蔽和難以防範。這不僅損害了受害者的利益，也對整個社會的信任體系造成了嚴重衝擊。

綜上所述，基於人工智慧的新型犯罪對我國公共安全構成了嚴重威脅。為了應對這些威脅，我們需要加強立法、監管和技術防範等方面的綜合措施。首先，完善相關法律法規和政策框架，明確人工智慧技術的合法應用範圍和監管要求。其次，加強監管力度，建立專門針對人工智慧技術的監管機構和機制，對相關企業和平台進行嚴格審查和監管。此外，鼓勵科研機構和企業加強技術創新和研發，提高人工智慧技術的安全性和可控性。同時，加強國際合作與交流，共同打擊跨國性的人工智慧犯罪活動。通過這些措施的綜合應用，我們可以更好地保障我國公共安全和社會的穩定發展。

四、基於人工智慧的新型犯罪手法的應對策略

隨着人工智慧（AI）技術的快速發展，基於 AI 的新型犯罪手法不斷湧現，給個人、企業和社會帶來了嚴重的威脅。為了應對這些挑戰，我們需要採取綜合性的應對策略，包括技術層面、法律和政策層面，以及教育和意識層面。

（一）技術層面的應對策略

1. 加強人工智慧的安全研究和開發

應對基於人工智慧的犯罪行為，技術層面的應對策略是至關重要的。首先，應加強人工智慧的安全研究和開發，投入更多的資源進行人工智慧安全演算法和技術的研發。這包括機器學習、深度學習、自然語言處理等技術的應用和研究，以增強對新型犯罪手法的檢測和防範能力。通過研發更高效的安全演算法和工具，可以更好地識別和應對網絡攻擊、惡意軟體、網絡釣魚等威脅。[9] 我國亦能夠參考目前國際上現有的做法，比如：美國國防高等研究計劃署（DARPA）啟動的 AI Next 專案，設立專門的 AI 安全研究中心，旨在集中力量攻關 AI 安全技術。

2. 建立人工智慧安全標準

在規範人工智慧技術的安全使用方面，應建立人工智慧安全標準。這包括制定和推廣數據安全、隱私保護、演算法透明度等方面的標準，以確保人工智慧系統的可靠性和安全性。例如，我國可參考國際標準組織（ISO、IEEE）所訂立 AI 安全規則，結合國內自身情況，制定符合國情的 AI 安全標準。通過制定統一的安全標準，可以引導企業和技術開發者遵循共同的安全準則，降低安全風險。

3. 加強國際合作與交流

應對基於人工智慧的犯罪行為需要全球範圍內的合作與交流。各國政府、企業、研究機構應加強國際合作與交流，共同研究和應對基於人工智慧的犯罪行為。例如，我國定期派遣相關機構人員參與 AI for Good Global Summit，此由國際電信聯盟（ITU）主辦，旨在促進全球範圍內的 AI 技術合作與交流會議。通過分享經驗、最佳實踐和技術成果，可以促進技術創新和防止新型犯罪的擴散。國際合作與交流還可以促進跨國執法合作，加強信息共用和聯合行動，共同打擊跨國犯罪。

（二）法律和政策層面的應對策略

1. 完善法律法規

為了確保人工智慧技術的合法、合規使用，政府需要制定和完善相關的法律法規。這包括數據保護法、網絡安全法、隱私法等法律檔的修訂和完善，以確保個人隱私和數據安全得到充分保護。通過明確人工智慧技術的合法應用範圍和監管要求，可以規範相關行業的行為，防止被用於非法目的。

在數據保護法方面，應加強對個人數據的保護，明確數據的收集、存儲、處理和使用的規範，防止數據被濫用或洩露。在網絡安全法方面，應加強對網絡系統的安全保護，防止網絡攻擊和數據洩露，保障網

[9] 王琦：〈生成式人工智慧（AIGC）犯罪風險及因應研究〉，《公安研究》，2023 年，第 9 期，第 19–24 頁。

絡系統的正常運行。在隱私法方面，應加強對個人隱私的保護，防止個人隱私被侵犯或洩露。例如，我國可參考歐盟的《通用數據保護條例》(GDPR)，其對數據保護和隱私提出了嚴格要求，為 AI 技術的應用提供了法律保障。

2. 加強監管力度

政府應建立專門的監管機構和機制，對人工智慧技術的使用進行嚴格監管。這包括對人工智慧系統的安全性進行評估和審查，以及對違法行為的調查和處罰。通過加強對人工智慧技術的監管，可以及時發現和預防潛在的安全風險，防止被用於非法目的。

監管機構可以對人工智慧系統的安全性進行評估和審查，確保其符合相關標準和規範。對於不符合規範的人工智慧應用，應進行限制和整改，以防止其被用於非法目的。同時，監管機構應對違法行為進行調查和處罰，對違法者起到震懾作用。可以借鏡鄰近地區，新加坡早於 2019 年推出人工智慧監管機構，當時考慮到星國大選將至，期間或有別有居心者濫用科技操作敏感的政治議題。此舉成功針對 AI 生成的政治相關內容採取措施及立法。

3. 制定國際合作協議

由於基於人工智慧的犯罪行為往往具有跨國性，因此政府應與國際社會簽訂國際合作協議，共同打擊基於人工智慧的犯罪行為。通過跨國合作和信息共用，可以加強執法力度和打擊犯罪的效果。國際合作協議可以包括情報交換、技術交流、聯合調查等方面的合作內容，共同應對跨國犯罪的挑戰。例如，參考《布達佩斯網路犯罪公約》，該公約促進了各國在打擊網路犯罪方面的合作，為 AI 技術的國際合作提供了借鑑。

(三)教育和意識層面的應對策略

1. 提高公眾的數字素養

公眾對數字技術和網絡的理解和認識不足，容易成為網絡犯罪的受害者。因此，推廣數字素養教育專案，教導公眾如何安全地使用互聯網、識別網絡威脅、保護個人隱私等是至關重要的。可以通過線上和線下的課程、宣傳資料、社區活動等方式，使公眾了解新型犯罪手法的形式和應對方法。例如，新加坡政府發起 AI for Everyone，通過舉辦講座和工作坊，提高 AI 相關知識的普及，為公眾提供基礎 AI 知識的免費課程。

2. 加強青少年的網絡安全教育

青少年是網絡使用的主要群體之一，也是網絡犯罪的高發人群。因此，針對青少年的網絡安全教育尤為重要。學校和社區可以開設網絡安全教育課程，教授他們如何安全上網、識別網絡陷阱、避免網絡欺凌等知識。同時，家庭也應該積極參與孩子的網絡安全教育，培養他們的安全意識和習慣。例如，警察部門防罪滅罪的宣傳，適時引入的 AI 犯罪的形式和手段等內容，從而提高青少年對 AI 犯罪的警戒心。

3. 促進企業和組織的內部培訓

企業和組織應該加強對員工的網絡安全培訓和教育，提高員工的防範意識和技能。培訓內容可以包括基本的網絡安全知識、識別網絡攻擊的方法、保護敏感數據和客戶信息的措施等。此外，企業還可以定期進行模擬攻擊和演練，提高員工應對網絡攻擊的能力和應急回應能力。例如，Google 公司的安全意識培訓。Google 定期為員工提供網路安全培訓，提高員工的安全意識和技能。

4. 加強公眾對倫理和隱私問題的關注

隨着人工智慧技術的普及，倫理和隱私問題越來越受到關注。政府、學術界和媒體應該加強宣傳和教育，讓公眾了解人工智慧技術可能帶來的倫理和隱私問題，以及如何應對這些問題。此外，應該鼓勵公眾參與相關政策的制定和監督，促進社會對倫理和隱私問題的關注和重視。[10]

[10] 翁傑、吳潔虹：〈利用 AI 變臉技術違法犯罪的應對對策〉，《廣東公安科技》，2020 年，第 28 卷，第 1 期。

綜上所述，應對基於人工智慧的新型犯罪手法需要全社會的共同努力。通過提高公眾的數字素養、加強青少年的網絡安全教育、促進企業和組織的內部培訓，以及加強公眾對倫理和隱私問題的關注，我們可以提高整個社會的網絡安全意識和防範能力，有效應對基於人工智慧的犯罪行為。同時，政府、企業和學術界也應該加強合作，共同研究和開發新的技術和方法，不斷完善網絡安全體系，為社會的穩定和發展提供保障。

五、結論與展望

在基於人工智慧的新型犯罪手法不斷湧現的背景下，本論文旨在探討應對這一挑戰的策略，並提供相應的建議和措施。通過對法律和政策層面、技術層面，以及教育和意識層面的應對策略進行分析和討論，我們得出以下結論：

首先，法律和政策層面的應對策略在打擊基於人工智慧的新型犯罪中起着重要的作用。制定和完善相關法律和法規對於規範人工智慧的應用和打擊犯罪至關重要。跨國合作和信息共用也是打擊跨國犯罪網絡的關鍵。此外，加強公眾的意識和教育也是法律和政策層面應對策略的重要組成部分。通過推廣數字素養教育專案和加強青少年的網絡安全教育，可以提高公眾對基於人工智慧犯罪的認識和防範能力。其次，技術層面的應對策略在預防和應對基於人工智慧的新型犯罪方面具有重要意義。技術創新在提高網絡安全和打擊犯罪方面發揮着關鍵作用。網絡安全技術的發展可以提高網絡系統的安全性和防禦能力，數據分析和監測技術可以幫助發現和預防犯罪行為。此外，人工智慧演算法和模型的設計也是技術層面應對策略的重要組成部分，通過提高檢測和預防犯罪的能力，有效應對基於人工智慧的新型犯罪。再者，教育和意識層面的應對策略在提高公眾防範能力和應對基於人工智慧的犯罪方面起着重要作用。提高公眾的數字素養和網絡安全意識是應對策略中的關鍵環節。通過推廣數字素養教育專案和加強青少年的網絡安全教育，可以培養公眾良好的網絡安全習慣和技能。同時，企業和組織內部培訓也是教育和意識層面應對策略的重要組成部分，通過提高員工的網絡安全意識和知識水平，可以降低組織遭受網絡攻擊和數據洩露的風險。

然而，應對基於人工智慧的新型犯罪仍面臨一些挑戰。首先，技術進步的速度遠遠超過了法律法規的制定和改進，需要加強法律制度的適應性和靈活性。其次，隨着人工智慧的發展，新型犯罪手法也在不斷演進，需要持續的研究和創新來應對新挑戰。此外，國際合作的加強也是應對跨國犯罪的重要手段，需要建立更加廣泛和深入的合作機制。

展望未來，我們可以從以下幾個方面繼續深入研究和發展：

第一，進一步完善法律和政策框架，以更好地應對基於人工智慧的新型犯罪。需要加強國家和國際層面的合作，制定更加綜合和適應性強的法律法規，以確保人工智慧的合法和道德使用。第二，繼續推動網絡安全技術和人工智慧演算法的創新，以提高對基於人工智慧的新型犯罪的防範和打擊能力。需要加強對網絡系統的安全設計和防禦能力的研究，同時提高人工智慧演算法的智能化和自適應性。第三，加強公眾的數字素養和網絡安全教育，提高公眾的防範能力和意識水平。需要通過多種渠道和途徑，推廣數字素養教育專案，加強青少年的網絡安全教育，提高公眾對基於人工智慧的犯罪的認識和防範能力。最後，加強國際合作和信息共用，建立更加廣泛和深入的合作機制。跨國犯罪往往具有複雜的網絡結構和組織形式，需要各國加強合作，分享情報和經驗，共同打擊跨國犯罪網絡。

綜上所述，應對基於人工智慧的新型犯罪手法是一個複雜而重要的任務。只有通過法律和政策層面、技術層面，以及教育和意識層面的綜合應對策略，才能有效應對和防範基於人工智慧的新型犯罪。此外，我們需要不斷研究和創新，加強國際合作，共同應對這一挑戰，以保護社會安全和公眾利益。

澳門保安範疇智慧雲警務數據治理的現狀分析及改善意見

王少嶺 *

摘要：保安當局貫徹科技強警的施政理念，期望透過智慧警務各項應用，提升本澳治安管理和監察的能力。智慧應用以數據為資源，數據需要通過治理，才能挖掘潛藏其中的價值，賦能智慧警務各項應用。本文首先介紹了數據治理的概念，以及數據治理相關理論框架。接着，總結澳門保安範疇智慧雲警務數據治理的現況及成效，保安當局成立了智慧雲警務的領導小組及數據治理小組、制定了智慧警務的五年規劃和制定若干標準規範、初步梳理數據資源及建設警務數據資源服務共享平台。最後，指出現時保安範疇智慧雲警務數據治理仍處於初步階段，需評估數據治理現況，制定針對性改善規劃，羅列6項智慧警務數據治理的困難及挑戰，並提出8項改善建議及展望。

關鍵詞：數據治理　數據管理　數據　智慧警務

Analysis of the Current Situation and Suggestions for Improvement in Smart Cloud Policing Data Governance in Macao's Security Sector

Wong Sio Leng

Abstract: The security authorities implement the governance philosophy of strengthening the police through technology, aiming to enhance Macao's security management and supervision capabilities through various smart policing applications. Smart applications leverage data as a resource, which needs to be governed to uncover its hidden value and empower various smart policing applications. This article begins by introducing the concept of data governance and its relevant theoretical framework. It then summarizes the current status and effectiveness of smart cloud policing data governance in Macao's security sector. The security authorities established a leadership team and a data governance team for smart cloud policing, formulated a five-year plan for smart policing, set several standards and specifications, conducted an initial analysis of data resources, and built a shared platform for policing data resource services. Lastly, the article highlights that smart cloud policing data governance in the current security sector is still in its initial stage. It is necessary to assess the current state of data governance and develop targeted improvement plans. The article identifies six challenges and difficulties in smart policing data governance, and proposes eight suggestions for improvements and future prospects.

Keywords: Data Governance; Data Management; Data; Smart Policing

*　王少嶺，警察總局情報分析中心警司，公共管理碩士。

一、前言

早在遠古時期，人類便以結繩記事等方式記錄數據，這亦是人類發展出智能的關鍵因素之一。工業革命以降，隨着電腦、互聯網、雲端平台、萬物互聯、人工智能、區塊鏈等一波波的技術革新，人類收集及記錄數據的技術得到長足的發展，所收集的數據類型及數量達到前所未有的程度，由以往缺乏數據，霎時進入資訊爆炸時代，大數據治理課題應運而生，如何將數據作為資產，發掘數據的價值，更是當前各國各行各業急切解決之課題。

澳門特別行政區政府早於 2016 年發表《澳門特別行政區五年發展規劃 (2016–2020 年)》，規劃中提出構建“智慧城市”和發展“智慧政務”，整合和共享政府內部的數據及其他各種資源，優化服務流程。及後，於 2019 年 5 月設立跨部門的專責小組——公共服務與數據治理專責小組，以統籌、協調並落實相關工作，建立完善的數據治理機制，推動跨部門的協作，解決資訊孤島對市民大眾以至各部門服務的負面影響，從而提升特區政府政務管理的效率和公共服務的水平。

二、數據治理概述

數據是人們對客觀事物的邏輯歸納之記錄，用於表示客觀事物的原始狀況。數據有很多種，例如數字、文字、圖像、聲音等等。“數據 (data)”更為着眼事物的原始情況，而“數據 (data)”則經過分析、歸納等處理後稱為“資訊 (information)”，從資訊再加以分析後謂之“知識 (knowledge)”，再通過不斷地行動與驗證，逐漸形成“智慧 (wisdom)”。就數據載體而言，可以是結繩、泥板、木刻、石雕、青銅器、紙張等等，現時大量的數據以電子形式儲存，下文所指的數據，正是特指這類電子數據。

當前大數據時代下，數據作為一項資產漸為人們所接受及重視，相較其他資產，數據資產具有虛擬性、增值性、時效性、共享性、安全性 5 項特徵[1] (圖 1)，這 5 項特徵中的核心是共享性和增值性。由於時效性的特質，以及數據的邊際成本小，因而共享具有新鮮度的數據更能發揮數據價值。有效的數據治理是從大數據提煉出數據資產的必要條件。

圖1　數據資產的五大特性

(一) 數據治理的起源及發展

1. 早期探索階段

數據治理在國外發展較早，早在 1988 年由 Richard Y. Wang 及 Stuart Madnick 共同倡議全面資料質量管理 (TDQM，Total Data Quality Management) 並於 90 年代初期，在麻省理工學院建立 TDQM

[1]　段效亮主編：《企業數據治理那些事》，機械工業出版社，2020 年，第 42 頁。

Research Program。同年，國際數據管理協會（Data Management Association，下稱 DAMA）成立，可以認為是現代數據治理的雛形。

直到 2002 年 Hugh J. Watson，Celia Fuller 及 Thilini Ariyachandra 共同發表題為《數據倉庫治理》的研究（Data warehourse governance: best practices at Blue Cross and Blue Shield of North Carolina），此為數據治理的概念首次出現在學術界。

2. 理論研究階段

2003 年國際數據治理研究所（Data Governance Institute，下稱 DGI）成立，與 ISO 國際標準化組織對數據管理與數據治理進行定義，DAMA 先後於 2009 年及 2017 年發佈 DMBOK《數據管理知識體系指南》第一版及第二版，至此數據治理已有成熟的框架。

3. 廣泛應用階段

近年，數據治理在我國得到廣泛的推廣及實踐，我國代表在 2015 年巴西聖保羅召開的 SC40/WG1 第三次工作組會議上提出了《數據治理白皮書》國際標準研究報告，主要內容有：數據是一種資產，以及提出數據治理模型。有關理念獲得與會者認同，並且由中國國家委員會參與編輯 ISO 38505。

2018 年，國家市場監督管理總局和國家標準化管理委員會發佈《中華人民共和國國家標準公告（2018 年第 9 號）》，批准《資訊技術服務治理第 5 部分：數據治理規範》。

由於業務需求及客觀條件，數據治理在金融業界和電訊行業發展較早，中國銀行保險監督管理委員會在 2018 年發布了《銀行業金融機構數據治理指引》。

（二）數據治理的定義

由於各個機構和個人對數據治理（Data Governance，簡稱 DG）的切入點和側重點有所不同，目前尚未形成一個統一標準並為各界所接受的定義。以下介紹業界權威機構、網絡百科及我國學者對數據治理的定義。

國際數據管理協會（DAMA）定義數據治理是指對數據資產管理行使權力和控制的活動集合（規劃、監督和執行）。國際數據治理研究所（DGI）定義數據治理是一個通過一系列資訊相關的過程來實現決策權和職責分工的系統。MBA 智庫百科、百度百科定義數據治理是組織中涉及數據使用的一整套管理行為，由企業數據治理部門發起並推行，關於如何制定和實施針對整個企業內部數據的商業應用和技術管理的一系列政策和流程。我國學者段效亮則認為（企業）數據治理是指從使用零散數據變為使用統一規範數據，從具有很少或沒有組織和流程治理到企業範圍內的綜合數據治理，從嘗試處理數據混亂狀況到數據井井有條的一個過程。

為加深對數據治理概念的理解，需與數據管理進行比較分析。數據管理與數據治理息息相關及意義相近，國際數據管理協會（DAMA）認為數據管理（Data Management）是為了交付、控制、保護並提升數據和資訊資產的價值，在其整個生命周期中制訂計劃、制度、規程和實踐活動，並執行和監督的過程。將數據治理和數據管理兩者的內涵和外延作比較，有三種觀點，一是認為數據管理（DM）是長期管控的過程，屬長效機制；數據治理（DG）是某一時間段對數據的臨時梳理措施和行為，針對數據質量，此觀點下，數據管理是包含數據治理的。二是認為數據治理是包含數據管理的，數據管理是數據治理的技術實現。三是認為數據治理和數據管理基本等同。

（三）數據治理的框架

數據治理的框架通常包括了政策制度、技術工具、數據標準、流程規範、監督及考核等方面，各個理論框架各具特色和優勢，以下介紹兩個較具代表性的框架。

1. 國際標準化組織 ISO38500 及 ISO38505 治理框架 (2008 年及 2017 年)

國際標準組織於 2008 年推出第一個 IT 治理的國際標準：ISO38500 (IT Governance)，標誌着資訊化正式進入 IT 治理時代，ISO38500 提出的 IT 治理框架（包括目標、原則和模型）同樣適用於數據治理領域。

隨後在 2015 年巴西會議上，中國代表團正式提出數據治理的新工作項目建議，得到國際與會專家的一致通過。根據該項建議，將數據治理國際標準更新為 ISO38505 (Data Governance)，並分為兩個部分：ISO38505–1《基於 ISO/IEC38500 的數據治理》和 ISO38505–2《數據治理對數據管理的影響》。

ISO38505–1 旨在為治理主體提供原則、定義以及模型，以幫助治理主體評估、指導和監督其數據利用的過程。

在目標方面，ISO38505–1 除了提升數據價值外，還明確以合規和風險管理為治理目標。在原則方面，承襲 ISO38500 IT 治理框架 6 個原則，職責、戰略、獲取、績效、合規和人員行為，對數據治理決定具指導性作用。在模型方面，治理主體應運用評估 (Evaluate)、指導 (Direct)、監督 (Monitor) 的 EDM 模型來開展數據治理工作，如下圖（圖 2）所示：

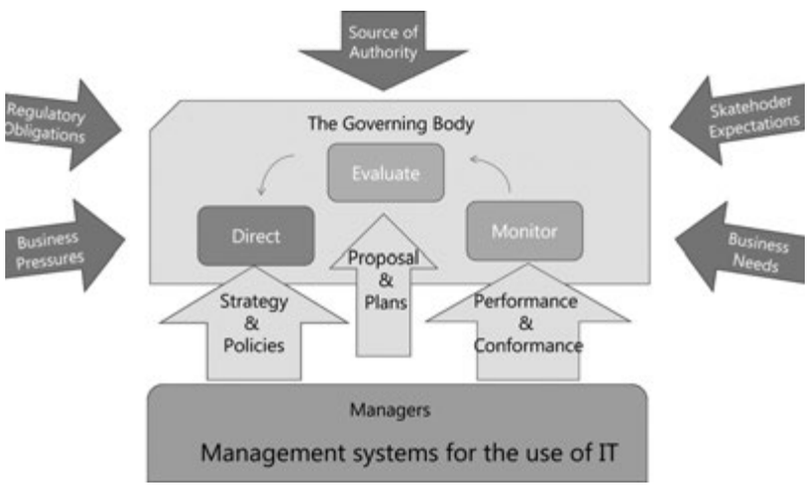

圖2 ISO 38505–1 EDM模型

2. 國際數據管理協會 (DAMA) 數據治理框架 (2017 年第二版)

DAMA 在《DAMA 指南第二版》首先總結了數據管理的 11 項職能，包括數據治理、數據架構、數據模型與設計、數據存儲與操作、數據安全、數據集成與互操作性、文件和內容管理、參考數據和主數據、數據倉庫和商務智能、元數據、數據質量管理，並把數據治理放在核心位置，並詳細闡述了數據治理的 7 項環境要素，即目標和原則、活動、主要交付物、角色和責任、技術、實踐和方法、組織和文化，每項數據職能領域都在 7 項環境要素約束下開展工作。建立兩個子框架構成：數據管理框架 DAMA 車輪圖（圖 3）及環境因素六邊形圖（圖 4）。

數據管理框架 DAMA 車輪圖將數據治理放在數據管理活動的中心，其他知識領域（數據體系結構、數據建模等）圍繞數據治理開展。

環境因素六邊形圖顯示了人、過程和技術之間的關係。它將目標和原則放在中心，這些目標和原則指導組織如何執行活動及有效地使用工具進行數據管理。

兩子框架因全面性和邏輯清晰，被研究人員廣泛借鑑和引用。但應用數據治理框架時不能忽略行業的獨特性，所以在實際應用上，要針對行業特徵進行修改。DAMA 車輪圖經過若干發展及演變，發展出不同的變體，在此不作闡述。

圖 3　數據管理框架 DAMA 車輪圖

圖 4　環境因素六邊形圖

除上述國內外提出的兩個數據治理框架外，不少的企業、機構及學者亦提出各自的數據治理框架，因各自的觀點、角度及側重點不同，相關的框架林林總總、各具特點，即使各個治理框架之間存在一定的差異及矛盾，總體而言有兩個共通點，一是各個治理框架都認為，數據治理涉及組織的整體運作，並且需要長期持續執行，是一個螺旋上升的過程，二是從各個框架中，有三個方面大致共性的核心要素，一是在頂層規劃方面，核心要素包括成立專門的數據治理領導組織、訂立願景及戰略、制定配套法律規範及倫理守則；二是在操作層面，核心要素包括數據質量管理、數據生命周期管理、數據安全和隱私、數據架構、分類及元數據[2]管理；在支撐配套體系方面，核心要素包括標準規範、審計及日誌監控等。

三、本澳智慧警務數據治理現況及改善意見

早在 2018 年保安領域的施政報告中，保安當局便提出構建保安範疇智慧警務及大數據應用的施政方針，以期運用大數據技術協助分析資訊和科學決策，更有效地預防及打擊犯罪。

（一）本澳智慧警務體系架構及相關數據治理

1. 本澳智慧警務體系架構

張了了及許鴻英參考內地的經驗並結合本澳的實際情況，在〈本澳“智慧警務”的實踐與思考〉[3]一文中提出一套由四大橫向結構層和四大縱向保障體系所組成的“四橫四縱”智慧警務體系架構（圖 5）。

(1) 四大橫向結構層

第一層是感知層，是警務資訊的廣泛感知和採集，包括視頻裝置、傳感裝置、定位裝置等等。第二層是網絡層，是智慧警務的通訊網絡，包括警務專網、視頻物聯網、移動警務網、電子政務網、無線集群網、高速互聯網等。第三層是數據層，又稱平台層，是智慧警務的數據中心，表現為集中式的大數據平台和“警務雲”平台。數據層支持文字、圖像、影像、聲音、向量空間等多種數據結構和模型，對大量警務數據進行匯集、整合、清理、組織、存儲和處理。第四層是應用層，或稱業務層，是基於大數據、雲計算而建構的針對各類警務具體應用的資訊系統之整合。

(2) 四大縱向保障體系

四大保障體系是智慧警務的物質基礎及制度支撐，包括有法律政策保障、技術標準保障、資訊安全保障及運維管理保障。

[2]　元數據（Metadata）是用來描述數據的數據，例如：數據所有者、數據來源、分類等資訊。

[3]　張了了、許鴻英：〈本澳“智慧警務”的實踐與思考〉，《澳門警察》，2020 年，第 10 期，第 29 頁。

圖5 智慧警務“四橫四縱”體系架構

2. 智慧警務體系架構中之數據治理

數據治理貫通上述第一層至第四層，並涉及四個保障體系，從源頭收集數據到終端應用無不涉及數據治理。

在警務工作資訊化的過程中，警務部門大多會為特定的事項開發針對性的系統，系統與系統之間的資訊交換往往欠缺統一的設計，導致資料間缺乏關聯性，資料庫之間的相互封閉，導致數據互不相通，形成“數據孤島”，需要通過對各系統的數據進行標準化清洗後，才能以統一的標準格式將數據匯聚到警務數據中心進行運算。

警務數據具有多源異構的特點，“多源”是指數據來源多樣；“異構”是指來源數據結構的差異性，涉及結構化、半結構化和非結構化數據，如數據庫表、XML 文件、各類文檔、音頻、視頻、圖片等。由於涉及範疇多樣且量大，所以警務數據涉及大數據處理，並且部分數據更新頻率較高，因而對數據治理要求較高。

智慧警務體系架構中之數據治理主要涉及在數據層（即平台層）建立“警務數據中心”。警務數據中心的作用是匯聚保安範疇各部門的警務資料，通過對數據進行治理，提高數據質量，供應用層使用，這一過程涉及大量繁複的數據治理。

（二）智慧警務數據治理的現況

1. 本澳警務範疇數據治理的頂層規劃

正如前文所述，數據治理涉及組織方方面面的整體運作，其中頂層規劃尤為重要，以下簡介保安範疇智慧警務數據治理頂層規劃的沿革。

(1) 數據治理領導組織

為推動智慧警務的建設，保安當局於 2018 年成立智慧警務跨部門工作小組，由保安司司長擔任組長、警察總局局長及保安司司長辦公室主任為副組長，各保安部隊及部門領導、主管及技術人員為成員，由警察總局局長負責統籌小組進行頂層規劃、框架設計、短中長期計劃，以及項目推進等工作[4]。在規劃智慧警務的過程中，亦牽涉到數據治理的規劃建設，故亦可視之為數據治理的領導組織。

智慧警務在系統建設、數據治理及系統落地使用等方面存在不少困難及挑戰，參考內地經驗、本澳相關研究並按保安範疇實際需要，保安當局於 2020 年第三季成立“數據治理小組”。數據治理小組組長由警

[4] 澳門保安司司長辦公室：〈2018 年度保安範疇施政方針的執行情況〉，《保安範疇施政方針》，網址：https://www.gss.gov.mo/cht/lag2019.aspx，2022 年 3 月 1 日。

察總局一名局長助理擔任，組員包括有參與智慧雲警務計劃的部門一名副局長，負責輔助保安司和智慧警務領導組織就智慧警務中數據治理的規劃、審議工作，牽頭構建相關數據資源共享平台，並推動數據的共享及使用。

(2) 願景及戰略

保安當局於 2018 年的《保安範疇施政方針》已指出保安當局智慧警務的目標和方向，逐漸由執法行動轉變為執法預警，由事後處理轉變為事前預防，使警隊進一步掌握執法上的主動性，強化對各類犯罪，包括恐怖主義犯罪和網絡攻擊的預警、防範及應對。本文認為保安範疇數據治理的願景是貫徹科技強警的施政理念，期望透過數據治理，挖掘數據價值，賦能智慧警務各項應用，實現預防、預警、預測，從而提升本澳治安管理和監察的能力。

戰略方面，保安當局制定了五年的智慧警務規劃，分三個階段，第一階段是 2019 年的基礎建設階段，建立警務數據中心和大數據綜合平台，以數據融合支撐實戰；第二階段是 2020 年至 2021 年的應用建設階段，搭建數據雲平台，全面匯聚警務數據，統一管理數據服務；第三階段是 2022 年至 2023 年的深化應用階段，以智慧驅動、深度應用邁向智慧化。透過分階段建設推進落實智慧警務，於不同階段都有對應的數據治理重點任務，分別是於第一階段的基礎建設及初步梳理數據資源，於第二階段建立警務數據資源服務共享平台，於第三階段提升數據質量，挖掘數據價值，賦能智慧應用。

2. 配套法律規範及數據治理倫理守則

智慧警務的構建，無可避免涉及個人資料的收集，收集個人數據和保護個人私隱是天平的兩端，保安當局需依據法律收集及處理個人資料，以平衡兩者。

於 2019 年 12 月 13 日，警察總局就保安範疇“智慧雲警務 " 項目之先行先試的先導計劃中有關個人資料處理，尤其包括部門與部門之間的資料互聯、儲存、合規等自動化處理程序事宜，向個人資料保護辦公室（現為“個人資料保護局”）提出許可申請。及後，其於 2020 年 3 月 23 日發出第 03/A/2020/GPDP 號許可，有效期為 5 年。[5]

鑑於儘管有資料互聯許可，然而在收集及處理警務數據方面，仍受到法律規範限制，需要從法律層面賦權，因此從 2020 年第三季開始，保安當局研究修改現行法律規範以滿足實務需要，最終有關法律及行政法規分別於 2020 年 12 月及 2021 年 6 月完成修改。透過是次修法，警察總局按其職權法律有關規定，[6]、[7] 在其職責範圍內，具正當性和能力與相關保安部隊及其他保安部門的數據庫實現互聯。

通過上述頂層規劃的構建及逐步完善，為數據治理的長遠發展起着核心支撐作用。

3. 智慧警務數據治理成效

(1) 制定若干標準規範

操作層面及支撐配套體系方面，上述“數據治理小組”成立以來，在標準規範方面，制定了四份保安範疇智慧警務標準文件，涉及小組的組成及運作方式、數據的分類分級標準、數據的上雲和申請、警務帳戶管理等範疇，讓日後推進智慧雲警務應用項目時有標準規範可依。此外，“數據治理小組”成立後定期召開領導會議，普及數據治理理念，制訂及審議標準規範文件，商議及共識數據治理的工作計劃。

(2) 初步梳理數據資源，建設首期警務數據資源服務共享平台

為了落實智慧警務規劃，於 2019 年啟動分階段建設，直至 2021 年建立了保安範疇統一警務雲數據中心，為共用運算資源能力及網絡互聯互通打好基礎。在此基礎上，亦構建了警務數據資源服務共享平台，為數據整

[5] 個人資料保護辦公室（現為“個人資料保護局”）於 2020 年 3 月 23 日發出第 03/A/2020/GPDP 號許可，https://www.gpdp.gov.mo/file/Permission/03-A-2020-GPDP-TC.pdf，2022 年 3 月 10 日。

[6] 第 1/2001 號法律《澳門特別行政區警察總局》第二條第二款（四）項：“以包括資料互聯在內的任何合法方式搜集、分析、處理及發佈為履行職責所需的一切情報及資料；”。

[7] 第 5/2009 號行政法規《警察總局的組織及運作》第 12 條（四）項的規定：“統籌和協調保安範疇構建資訊互聯互通平台的工作，以確保與澳門特別行政區其他公共部門或實體所使用的資訊處理方法的兼容性；”。

合、治理、共享、交換，以及大數據應用提供了支撐，同時各部門亦結合共享數據推出各種相關應用系統。

DMBOK 金字塔（Aiken）框架[8]認為大數據治理從着手相關工作到能够挖掘數據價值需要經歷四個階段（圖 6），分別是：

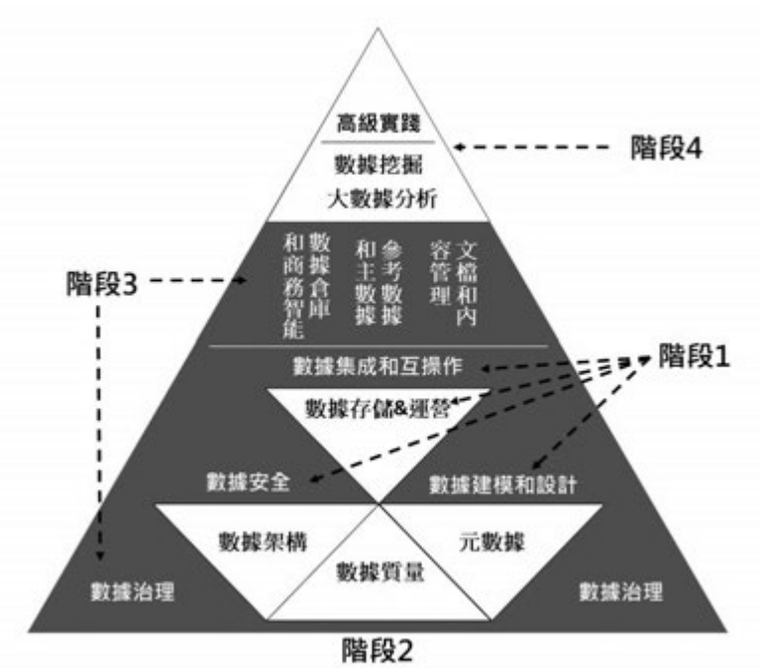

圖6 DMBOK金字塔（Aiken）

第 1 階段：組織購買包含數據庫功能的應用程序。這意味着組織以此作為數據建模、設計、數據存儲和數據安全的起點。

第 2 階段：組織開始使用應用程序，發現數據質量方面的挑戰。但獲得更高質量的數據取決於可靠的元數據和一致的數據架構。

第 3 階段：管理數據質量、元數據和架構需要嚴格地實踐數據治理，為數據管理活動提供體系性支持。

第 4 階段：組織充分利用了良好管理數據的好處，並提高了其分析能力。

本文認為現時本澳智慧警務的數據治理處於初步完成第 2 階段，正邁入第 3 階段，而這一階段正正是能否實現高級實踐（例如智慧化應用）的關鍵階段，需要着手大量繁複的數據治理工作，尤其管理數據質量、元數據管理等等。

4. 本澳智慧警務數據治理的困難及挑戰

(1) 涉及數據數量大、多源、異構

粗略估計數據治理工作將覆蓋數十個資訊系統和數百個數據表，而警務數據量大、多源、異構，各系統之間缺乏統一的規劃，需對各資料庫的結構和模型進行探查、辨認、分析，確定數據之間的邏輯聯繫和依賴關係，最終，經過對現有大量資料庫的分析和重整，構建一套標準化、統一、集中的資料庫結構，將來自各保安部門的警務數據連成一體、融會貫通，完成構建一個共享的警務數據中心。由於相關的工作量相當巨大，需要按輕重緩急分階段建設，現時只是進行了初步的數據治理，以及構建了警務數據資源服務共享平台，由於尚未建立統一的數據標準，元數據及主數據管理亦未盡完善，令智慧應用的推進舉步維艱。

[8] DAMA 國際著，DAMA 中國分會翻譯組譯：《DAMA–DMBOK2 DAMA 數據管理知識體系指南》（電子書），機械工業出版社，2020 年，第 87 頁。

(2) 缺乏相關工作經驗，沒有前例可循

大數據治理涉及前沿的科技應用，相關的技術不單新穎複雜，而且系統架構龐大，保安當局在規劃推進時，缺乏相關工作經驗，亦沒有前例可循。

(3) 數據治理系統需高度客制化，溝通協調及對接繁複

數據治理業界供應商為數不少，相關數據治理系統亦林林總總，但各個組織的數據治理有其特殊性，本澳與鄰近地區無論是法律制度，還是具體警務工作均有所不同，再者警務工作與一般企業甚至其他政府部門對處理數據的需求亦有所不同，導致無法直接使用現成的數據治理系統，需要配合本地化需求進行定制化，部分改動或涉及系統的底層設計，這對供應商的客制化能力要求較高。

在定制的過程中，需要警方的業務人員及技術人員參與，亦涉及不同供應商之間的系統對接，當中的溝通協調及對接調校困難及繁複。

(4) 系統治理功能尚待完善，數據質量有待提升

數據治理工作貫穿整個“智慧雲警務”四個橫向層，警務數據資源服務共享平台是智慧警務中平台層核心項目之一，對上作為應用層的基礎，提供各項數據服務；對下則負責整合來自網絡層和感知層的數據。雖然資源服務共享平台已於 2021 年正式推出，唯數據治理的工作並非一蹴而就，受限於人力、物力及數據標準化的工作未夠徹底，數據質量有待提升，平台的操作及核心功能尚待完善。

(5) 數據治理需複合型人才

進行數據治理工作時需要具有檢視、分析及構建數據表能力及相關專業知識，當中涉及不少數據應用及數據治理概念，如：數據標準化、數據定級、標籤應用、建模等。人員除了要掌握上述概念外，還要了解相關概念之應用、處理及操作流程，再結合自身業務之運作經驗，才能對數據作出分析，並將之轉化為實際應用。由此可見，數據治理的工作具一定的複雜性及跨領域，這類複合型人才需時培養。

(6) 疫情影響

因疫情關係，本澳於 2021 年 9 月 24 日至 10 月 15 日，以及 2022 年 6 月 19 日至 8 月 2 日，先後兩次進入即時預防狀態，特區政府開展了多次全民核酸檢測。保安範疇各部門全力參與防疫工作；另外，抗疫期間影響了保安部門之間以及保安部門與供應商之間的會面及交流；此外，由於網絡安全的原因，相關系統設於內網，供應商的技術人員亦無法透過遠程方式接入內網工作，影響系統的調試進度。上述情況均會影響數據治理的工作進度。

5. 智慧警務數據治理改善建議及展望

現時保安當局已完成了初步的數據治理，包括成立了智慧雲警務的領導小組及數據治理小組、制定了智慧警務的五年規劃、制定若干標準規範、初步梳理數據資源及建設警務數據資源服務共享平台。

參考上文 DMBOK 金字塔（Aiken）框架（圖 6），組織由進行數據治理到良好管理分為 4 個階段，本文認為澳門智慧警務的數據治理處於初步完成第 2 階段，正邁入第 3 階段，而這一階段正正是能否實現高級實踐（例如智慧化應用）的關鍵階段，需深化完善數據治理。為此，本文提出以下 8 點改善建議及展望：

(1) 評估數據治理現況，制定針對性改善規劃

進行數據治理現況評估是改善數據治理的第一步，可由保安當局或第三方作全面的排查調研，評估標準可以參考《DAMA 指南第二版》、國際標準、國家標準、行業標準及數據治理企業經驗等等。

以下介紹《DAMA 指南第二版》中的數據管理成熟度評估，該評估項目包括了十項數據管理的核心要素，分別是數據架構、數據建模、存儲和操作、數據安全、數據集成和互操作、文件和內容管理、參考數據和主數據、數據倉庫和商務智能、元數據及數據質量。每項要素評級由 0 級至 5 級，分別為無能力級、初始級、可重複級、已定義級、已管理級和優化級。以下圖 7 引用《DAMA 指南第二版》（電子書）第 954 頁的數據管理成熟度評估可視化示例（僅為舉例說明，並非對現況評估）。

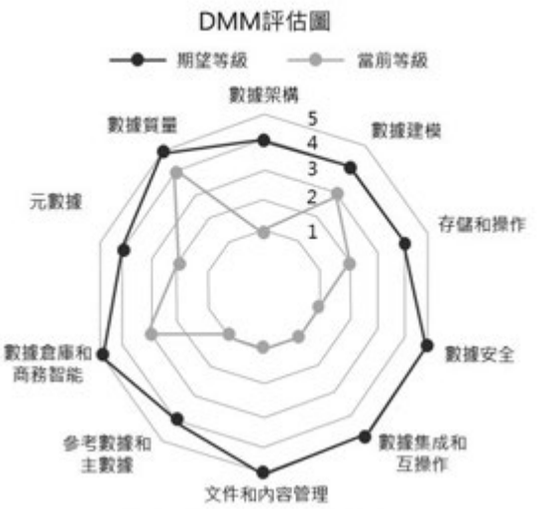

圖7 數據管理成熟度評估可視化示例(僅為舉例說明，並非對現況評估)

圖 7 直觀地呈現了數據管理成熟度評估的結果。針對十項核心要素的評估，圖形的外環顯示了組織理想應具備的能力等級，內環則顯示通過評估確定現時的能力等級，兩環之間距離最大的區域代表着組織面臨的最大風險。這樣的評估有助組織了解自身的短板，從而按輕重緩急確定優先事項，制訂有針對性的改進計劃，還可以用來測量一段時間內的進展情況，由核心到外圍，由可用到優化，由項目落地到項目治理，逐步完善。

(2) 強化數據治理小組組成，完善系統規劃及應用落地協調推進機制

現時數據治理小組主要成員為各部門的領導及主管，涵蓋業務及技術範疇，可就數據治理的上層規劃制定標準。然而，數據治理涉及大量跨領域的繁複工作，因此，除領導小組外，宜在操作層面也成立數據治理業務及技術小組，由不同範疇的人員共同參與，成員包括有業務人員、資訊技術人員、數據分析人員及應用開發人員。[9] 系統開發階段需要有業務人員充分參與，調試階段要設立定期的追蹤跟進機制，應用落地時需要推廣培訓。

(3) 制定數據標準，提升數據質量

數據治理涉及大量數據定標及處理工作，需要按輕重緩急分階段建設，由於現時尚未建立統一的數據標準，元數據及主數據管理亦未盡完善，令智慧應用的推進舉步維艱。

為此，宜成立跨部門的數據標準制定小組，由各部門的業務人員和技術人員與供應商共同參與，制定統一的警務數據標準和規範，為數據匯聚、數據交換及智慧應用打下基礎，現時已制定了數據分類、分級標準，下階段應着手數據字典、元數據標準、數據交換技術規範、數據傳輸協議及數據質量標準的制定。

(4) 提升及補充系統的數據管理功能

數據治理行業近年有長足的發展，治理工具業已有業界標準功能，涵蓋數據治理的各個環節，下階段需根據本澳實際需要，提升及補充系統的數據管理功能，尤其元數據管理、數據標準管理、主數據管理、數據質量管理、安全管理，以及數據生命周期管理，系統化及自動地對數據進行治理，確保數據在數據生命周期間之安全性、一致性、完整性及可用性，並對數據質量及存量作出管理及控制。

(5) 增設數據監控功能

為確保數據質量持續保持良好，數據治理項目實施後需要構建一個基於大數據行為分析的數據質量監測平台。平台需要具備實時探知數據質量的能力，並且把數據質量量化展現，同時提供問題數據處理的通道。

[9] 張了了、許鴻英：〈本澳“智慧警務”的實踐與思考〉，《澳門警察》，2020 年，第 10 期，第 38 頁。

通過圖表以可視化展現數據質量結果，數據運維管理人員可直觀地從多個角度充分了解到數據質量的狀況及演變過程，以便及時發現問題並實時處理，真正做到把控數據質量。

(6) 培養數據治理人才

數據治理是一項持續進行的螺旋上升過程，過程中可以借助供應商構建，同時亦需要建立自身的數據治理技術及業務團隊，掌握主導權。

進行數據治理工作時需要具有檢視、分析和構建數據表能力及相關專業知識，工作具一定的複雜性及跨領域，這類複合型人才需時培養。技術人員需要學習及掌握相關前沿的資訊技術，業務人員需要對相關技術原理有基本認識，以及對數據治理的理念有較深了解。

可以從四方面培養數據治理人才，首先，數據治理人員在工作過程中，應主動學習相關技術，累積相關知識，以實戰提升治理能力；其次，部門應針對數據治理不同階段的需要，以及數據治理不同崗位的特性，開設專門的課程、培訓班及講座；再次，可與行政公職局、保安部隊高等學校、其他高等院校或具資質機構合作舉辦相關培訓班；最後，鄰近地區數據治理業界近年有長足的發展，其相關經驗及技術均較本澳成熟，可組織本澳數據治理相關核心工作人員到鄰近地區警務部門或業界就數據治理方面作專項交流、培訓或考察。

(7) 加強警企合作

數據治理行業近年有長足的發展，相關治理產品亦林林總總，在選擇供應商時，除了看企業規模外，更要看企業數據治理部門的規模，相關產品功能，企業對產品的客制化能力，以及協調對接能力。

在系統開發的過程中，技術人員要主動了解系統背後的核心技術和相關原理，避免過於依賴供應商，掌握主導權。規劃階段應充分徵詢業務部門的意見，宜業務、技術及供應商三方共同參與系統的開發及調試，確保數據治理系統功能切合實務需要，以免系統落地後功能不對標，因而要再次調試。

(8) 擴大數據來源，預留對接擴展

收集個人數據和保護個人私隱是天平的兩端，而法律則是支撐兩端平衡的支點，保安當局就收集大數據作智慧化應用，應在法律許可下，按實務警務需要應取盡取。按現時的法律規定，警察總局在其職責範圍內，具正當性和能力收集相關保安部隊及部門的數據，而保安範疇以外的部門或機構的資料收集，需按照《個人資料保護法》、《打擊電腦犯罪法》、《網絡安全法》及部門或機構的職權法律及有關規定進行。另外，要充分利用智慧城市的大數據資源，同時亦需賦能智慧城市，為此需預留對接擴展。

四、結語

當今國內外形勢複雜多變，近年澳門博彩業結構調整，百年變局疊加世紀疫情，凡此種種對保安當局的治理能力帶來更大考驗。保安當局貫徹“科技強警”的施政理念，期望透過數據治理，挖掘數據價值，賦能智慧警務各項應用，實現預防、預警、預測，從而提升本澳治安管理和監察的能力。

保安當局現時完成了初步的數據治理，包括成立了智慧雲警務的領導小組及數據治理小組、制定了智慧警務第一個五年規劃和若干標準規範、初步梳理數據資源及建設警務數據資源服務共享平台。

按照 DMBOK 金字塔（Aiken）框架（圖 6），本文認為本澳智慧警務的數據治理處於初步完成第 2 階段，正邁入第 3 階段，而這一階段正正是能否實現高級實踐（例如智慧化應用）的關鍵階段，需深化完善數據治理。為此，本文提出八項改善建議及展望：1. 評估數據治理現況，制定針對性改善規劃；2. 強化數據治理小組組成，完善系統規劃及應用落地協調推進機制；3. 制定數據標準，提升數據質量；4. 提升及補充系統的數據管理功能；5. 增設數據監控功能；6. 培養數據治理人才；7. 加強警企合作；8. 擴大數據來源，預留對接擴展。數據治理是一個螺旋上升、持續進行的過程，需要持續推行 PDCA 迴圈，發掘數據價值，賦能智慧應用。

執法語言智能訓練系統在反詐預警勸阻領域的應用研究**

楊勇、陶魏光錫、鄧媛 *

摘要：電信網絡詐騙犯罪由於其作案手段的非接觸性和網絡犯罪的虛擬性，且缺少傳統意義上的物證載體，導致對其進行偵查打擊尤為困難。因此電信網絡詐騙的犯罪生態治理應當注重源頭治理，以犯罪預防為核心，從而在本源上降低發案率。電詐犯罪的預防分為預警和勸阻兩個部分，反詐預警以宣傳工作為主，而反詐勸阻主要是針對將要發生或是已經發生的詐騙案件進行人工干預。然而由於涉詐案件數量龐雜、基層警力資源不足、勸阻者和受害者之間的認知偏差等因素，預警勸阻工作往往難以取得顯著成效。本文通過分析當下反詐預警勸阻工作的難處，結合勸阻主體執法語言能力、勸阻話術、情景訓練技術、對話系統等要素，探究將執法語言智能訓練系統應用於反詐課程建設、反詐話術能力培訓、現場執法語言培訓的可行性，以此提高反詐預警勸阻主體業務素養、優化反詐業務工作。

關鍵詞：電信網絡詐騙　人工智慧　預警勸阻　執法語言訓練

Applied Research on the Intelligent Training System Based on Law Enforcement Language in the Field of Anti-Fraud Early Warning and Dissuasion

Yang Yong; Taowei Guangyang; Deng Yuan

Abstract: Owing to the non-contact and virtual nature of network crime and the lack of traditional material evidence, it is particularly difficult to investigate and crack down on telecom network fraud. Therefore, to reduce the incidence rate at the source, the ecological management of telecom network fraud crime should pay attention to the source management while crime prevention should also be the core. The prevention of electric fraud crime is divided into two parts: early warning and dissuasion. Anti-fraud early warning is mainly propaganda work, while anti-fraud dissuasion is mainly manual intervention for fraud cases that will happen or have already happened. However, due to the large number of fraud cases, the lack of police resources from the ordinary level and the differences in cognition between the dissuaders and the victims, it is often difficult to achieve significant results in early warning and dissuasion. By analyzing the current difficulties encountered in anti-fraud early warning and dissuasion, this paper explores the feasibility of applying the law enforcement language intelligent training system to the construction of anti-fraud courses, the training of anti-fraud skills and the on-site law enforcement language training by combining elements like the law enforcement language ability of the dissuasive body, the dissuasive speech technique, the situational training technique, the dialogue system, etc. so as to improve the quality of the work done by the anti-fraud early warning and dissuasive body in addition to optimizing the anti-fraud tasks.

Keywords: Telecom Network Fraud; Artificial Intelligence; Early Warning and Dissuasion; Law Enforcement Language Training

---

*　楊勇，廣東警官學院警務指揮戰術系講師。

*　陶魏光錫，廣東警官學院偵查系學生。

*　鄧媛，廣東警官學院警務指揮戰術系學生。

**　1.《警察現場執法語言智能輔助訓練系統研究》項目類別／編碼：廣東省教育科學規劃課題（高等教育專項）2023GXJK413，項目來源（下達單位）：廣東省教育科學規劃領導小組辦公室。2.《警察智能執法語言訓練系統教學設計研究》項目類別：高等教育教學改革，項目來源：廣東省本科高校教學質量與教學改革工程，下達單位：廣東省教育廳。

一、前言

電信網絡詐騙犯罪，是指行為人以非法佔有為目的，利用通信信息技術和手段實施詐騙的違法犯罪行為。[1] 在傳統的犯罪生態中，物證是犯罪信息的主要載體，犯罪信息表現為基於犯罪現場的物品與痕跡。[2] 而電詐犯罪由於其犯罪手段的非接觸性和網絡犯罪的虛擬性，導致其在傳統意義上的痕跡物證較為匱乏，同時作為一種新型犯罪，電信網絡詐騙的集團化、產業化特點突出，犯罪鏈條長、犯罪主體流動性強、參與人員眾多，打擊治理難以取得成效。[3] 因此針對電信網絡詐騙的犯罪治理應當注重源頭治理，從根源上降低案件的發案率，才能最大程度地減少其危害。

反詐預警勸阻屬於“預防端”治理，分為“預警”和“勸阻”兩個部分。反詐預警以宣傳工作為主，旨在增強群眾對涉詐行為的認知和心理預防效應；而反詐勸阻主要是對涉詐事件或案件進行人工干預，對可能正在遭受電信網絡詐騙的被害人進行阻斷，以防止造成損失，[4] 後者在時間上更具緊迫性。

反詐預警極度依賴宣傳攻勢和政策支持。在 2021 年 4 月，習近平總書記提出打擊治理電詐犯罪要強化系統觀念、法治思維，注重源頭治理、綜合治理，堅持齊抓共管、群防群治，[5] 致力形成“打防結合、預防為主”的新型網絡空間反詐治理模式。[6]2023 年 8 月，電影《孤注一擲》上映，極大程度加深了民眾對電詐犯罪的認知，全國電詐案件發案率斷崖式下降，但很快又觸底反彈，恢復至電影上映前的水平。反詐預警工作註定漫長且艱巨，其工作成效難以呈現在發案率的變化上，相較之下，反詐勸阻對即將或正在發生的涉詐行為直接進行阻斷攔截，治理效果更加顯著。

反詐勸阻工作分為電話勸阻和上門勸阻，二者均對勸阻主體的語言能力和話術技巧有着較高要求，而公安機關作為反詐勸阻的主要執行主體，對語言能力的考驗主要體現在執法語言能力上。公安民警執法語言能力是公安民警應具備的核心能力，[7] 其中包括執法用語和溝通用語。執法用語是民警在執法過程中依據相關法律法規、部門規章及規範性文件要求所表述的程式化的法律專業用語，[8] 溝通用語即為生活語言。[9]

反詐勸阻工作既需要規範化勸阻話術、專業金融知識，也需要察言觀色、穩定情緒、調節氛圍的溝通性語言。然而由於涉詐案件數量龐雜、基層警力資源不足、勸阻者和受害者之間的認知偏差等因素，公安民警現有的執法語言素養和業務效能難以取得顯著成果。此外，傳統的執法語言能力培訓由於較高的培訓成本和較長的培訓周期也導致了執法語言培訓次數少、強度低、實用性差。本文立足於反詐勸阻工作現存的問題，通過引入自然語言處理和人機對話系統，研究將 AI 訓練技術應用於公安民警執法語言素養、反詐話術技巧培訓以及反詐課程建設的可行性。

二、當前反詐勸阻工作存在的問題

（一）勸阻工作的問題與現狀

勸阻主體包括了基層民警、反詐偵防平台業務人員、警務輔助人員以及社區工作人員。很多警務人員在執行勸阻工作時，無法有效運用勸阻話術和執法語言，不能正確引用專業金融知識、法條和法律解釋，內容空洞，缺乏邏輯和條理。具體體現在勸阻過程中開口意願不高，語言表達能力差，表達不清、用詞不當等。個別警務人員在勸阻工作過程中手法過於生硬，語言過於隨意，僅僅將“止付”當做最終目的，以教條化的手段要求被害人終

[1] 王潔：〈電信網絡詐騙犯罪的獨特屬性與治理路徑〉，《中國人民公安大學學報（社會科學版）》，2019 年，第 35 卷，第 4 期，第 1–10 頁。

[2] 倪春樂、王泊勳：〈大數據驅動的偵查思維創新與實踐邏輯〉，《中國人民公安大學學報（社會科學版）》，2023 年，第 39 卷，第 2 期，第 71–82 頁。

[3] 王曉偉、趙照：〈電信網絡詐騙犯罪人員流的構成與偵查方法研究〉，《中國人民公安大學學報（社會科學版）》，2022 年，第 38 卷，第 4 期，第 53–64 頁。

[4] 徐舟、包涵：〈反詐預警勸阻機制的運行風險與完善路徑〉，《鐵道警察學院學報》，2023 年，第 33 卷，第 1 期，第 37–43 頁。

[5] 王君賢、張浩：〈電信網絡詐騙犯罪預警勸阻的現實意義問題檢視及發展路徑〉，《雲南警官學院學報》，2023 年，第 4 期，第 68–73 頁。

[6] 張壯：〈說服理論下電信網絡詐騙勸阻工作研究〉，《網絡空間安全》，2022 年，第 13 卷，第 3 期，第 101–106 頁。

[7] 馬加民、程天磊：〈公安民警執法現場語言控制規範化探究〉，《公安教育》，2022 年，第 5 期，第 30–34 頁。

[8] 陳士果：〈一線民警現場執法語言的訓練及使用原則〉，《廣州市公安管理幹部學院學報》，2016 年，第 26 卷，第 4 期，第 27–30 頁。

[9] 黨德強：〈芻議執法語言規範化與警察形象塑造〉，《河北公安警察職業學院學報》，2021 年，第 21 卷，第 2 期，第 5–8 頁。

止轉賬。這種工作模式忽視了被害人的底層認知問題，沒有落實“反洗腦”的要求，最終的結果往往不盡人意。

（二）警力資源與勸阻工作的矛盾

現階段的警力配置難以滿足實際工作和實際需求，龐大的勸阻工作量和極度稀少的警力資源使得高素質主體難以發揮效能。由於反詐警情數量龐雜，反詐勸阻工作一般通過電話勸阻的方式進行，上門勸阻主要針對情況緊急、涉案數額巨大的高危對象。由於涉詐警情數量龐雜，警力資源極其有限，因此電話勸阻和上門勸阻的比例高達 10:1。雖然勸阻主體範圍寬泛，但上門勸阻的大部分工作由社區工作人員和警務輔助人員完成。電話勸阻同樣困難重重，一個基層的反詐中隊每天撥打的勸阻電話高達數千例，平均下來每場通話時間不超過一分鐘。繁雜的勸阻工作和稀缺的警力資源導致公安機關在勸阻工作中無法發揮主體作用。

（三）勸阻話術與培訓問題

1. 未形成標準化話術體系

勸阻話術指的是預先準備好的專業性辭彙和勸告語言。由於現實的執法環境、勸阻情境複雜，民警很難現場構思語言，因此預先將話術知識爛熟於心，可以有效避免出現卡頓的情況，然而現階段的反詐勸阻尚未形成標準的話術體系。由於勸阻主體和處於被害狀態的被害人都存在不同程度的認知偏差，[10] 加上話術缺乏專業金融知識做支撐，口號式、宣傳性質的內容過多，反詐勸阻難以改變被害人的底層認知邏輯，效果不盡人意。

2. 未形成系統化訓練模式

培訓模式落後，授課內容過於理論、實用性差。傳統的執法語言培訓方式為“老帶新”的帶教模式，[11] 該模式的教學效果主要受授課方式和教育者自身的執法語言素養影響，沒有統一的語言規範和詳細的語言標準，也欠缺嚴謹、統一的考核評估標準。現階段各地的公安機關執法語言細則大多為綱領性規範，實用性和指導性欠佳。各單位、警種之間的內容繁複，甚至互相衝突，無法進行跨地域推廣，更無法形成標準化效應。

培訓周期長、成本高昂，訓練次數少。帶教模式需要對學員進行集中培訓和統一管理，培訓期間學員無法正常開展工作，培訓承辦方還需要負責學員的飲食和住宿。因此傳統的帶教培訓成本高昂、培訓周期較長，起效速度慢。執法語言實戰演練的次數和強度同樣有限，內容過於簡化、對抗強度不高，無法模擬真實的執法、勸阻情況，對學員的執法語言素養和話術能力的考察不徹底。

三、智能訓練系統定義

（一）系統概念

智能執法語言訓練系統是一款借助語音科技公司的軟體和前沿技術，將公安民警執法語言訓練內容納入教學培訓系統中，開發出的圍繞執法語言實戰訓練的電子輔助工具。該系統的訓練模式分為問答訓練和情景對練兩個部分，採用了智能語音問答交流的模式，融入了執法語言溝通技巧和法律條文；系統由專業的教官團隊設計情景問題及回答範本，這些問題來源於警察過往現場執法中高頻出現的詞句與各類典型案例事件。民警通過自主學習和大量練習，提高自我的使用執法語言能力。

（二）技術原理

1. 自然語言處理

自然語言處理技術常見於實驗室，通過運用相關統計學、機器學習演算法等理論與方式，完成科學處

[10] 何靜秋：〈電信網絡詐騙犯罪被害預防的治理困境與優化進路——基於虛假投資理財類案件的實證考察〉，《中國人民公安大學學報（社會科學版）》，2023 年，第 39 卷，第 4 期，第 83–96 頁。

[11] 韓國棟：〈論公安民警現場執法語言規範化建設〉，《中國人民警察大學學報》，2023 年，第 39 卷，第 9 期，第 51–56 頁。

理圖片、文本的任務，[12] 其英文全稱為“Natural Language Processing”，縮寫為“NLP”。NLP 的主要功能是實現人類語言和機器語言之間的相互轉化，是進行人機交互的重要媒介。

現階段 NLP 模型分為兩大類：迴圈神經網絡模型（RNN）和前饋神經網絡模型（FNN）。其中前饋神經網絡又稱“傳統神經網絡”，其層級結構通常為每層神經元與下一層神經元全連接，同層的神經元之間不存在連接。[13] 在 Transformer 發佈之前，FNN 模型在網絡結構上沒有環路或者回路，這意味著在數據集輸入系統時，同層級之間的數據沒有回饋連接和交互，這也導致模型的訓練成果往往不盡人意。

迴圈神經網絡的網絡結構為串聯式，在預設的神經元節點可將輸出結果再度導入運算模型，以保證模型各層級數據的依賴關係。因此迴圈神經網絡在處理序列模型時，其導出結果關聯度高、擬真效果好。但當文本較長時，其隱層顯得非常薄弱，存在較大不足，[14] 容易出現梯度消失和梯度爆炸現象，在處理長文本信息時反而不如 FNN 模型。

2. 智能對話系統

作為人機交互技術（Human Computer Interaction, HCI）的核心部分，人機對話系統（Human–Machine Dialogue System）相當於多個機器語言演算法技術的集大成者，旨在儘可能地利用機器語言去模擬人類語言，從而使人類和電腦之間的交流互動更加自然、流暢且真實。一個完整的任務型對話系統包括 5 個部分：[15] 自然語言理解（NLU）、自動語音識別（ASR）、對話管理（DM）、自然語言生成（NLG），以及語音合成（TTS）。這其中對話管理（DM）又包括了對話策略（Dialogue Policy, DP）和對話狀態跟蹤（Dialogue State Tracking, DST）。

人機對話系統的發展主要分為三個階段：第一階段是基於符號規則和範本的原始對話系統，第二階段是基於機器學習程式的對話系統，第三階段則是基於數據驅動和深度學習機制的對話系統。對話系統的學習深度和通用性取得長足進步，這使得第三代對話系統除了用準確、簡潔的人類語言回答問題外，更注重與人的交互、對人意圖的理解、對對話氛圍的感知，以及回答的多樣性和個性化，以此獲得擬真度更高的交互體驗。

四、系統在反詐課程中的應用

（一）反詐課程開發

1. 反詐課程題庫

課程題庫是學員進行執法語言訓練和執法語言能力考核的依據，主要分為問答題庫、情景題庫、話術清單三大模組，分別用於學員的快問快答訓練、情景對話訓練和反詐話術訓練。教師需要在系統後台根據課程和題庫類型，設立相關的問題和標準答案，系統會根據學員的音頻轉寫文本進行關鍵字、敏感詞和話術準確度檢測，並以此為評分依據。教師可以將學習檔導入資料庫，經人工審核完畢後，系統將自動生成電子卡片供學員閱覽。此外，系統也支持將已錄入的問答題庫數據導出，教師在後台可直接通過系統鏈接下載。

2. 勸阻課程分類

教師在新增問答訓練題庫時，需要根據對話訓練的問題和答案判斷屬於哪個分類，學員通過選擇不同類型的題目以達到對應的訓練目的。問答題庫根據當前公安業務工作分為危機談判訓練、反詐話術技巧訓練、戰術語言訓練、政治素養訓練、執法溝通訓練等多個類型的課程。反詐勸阻工作因應不同類型的詐騙手段分為多種類型的勸阻話術，常見的有刷單類詐騙勸阻、貸款類詐騙勸阻、冒充客服類詐騙勸阻和冒充公

[12] 葉符明：〈深度學習在自然語言處理 NLP 中的應用研究〉，《信息記錄材料》，2021 年，第 22 卷，第 11 期，第 148–149 頁。

[13] 楊麗、吳雨茜、王俊麗等：〈迴圈神經網絡研究綜述〉，《電腦應用》，2018 年，第 38 卷，第 S2 期，第 1–6 頁、第 26 頁。

[14] 柳秀秀、孔春偉：〈自然語言處理在金融領域應用的場景、挑戰和發展建議〉，《金融科技時代》，2023 年，第 31 卷，第 5 期，第 23–27 頁。

[15] 趙陽洋、王振宇、王佩等：〈任務型對話系統研究綜述〉，《電腦學報》，2020 年，第 43 卷，第 10 期，第 1862–1896 頁。

檢法類詐騙勸阻，專業課程的分類就是依照以上的門類標準。在定製反詐勸阻能力訓練題庫時，需要將預設問答內容進行定性和區分，選擇正確的課程類型。

3. 標準問題答案

設立標準問法和標準答案是問答訓練和核心部分。通常一個提問和一個答案為一組問答，一道題由一組問答構成。設立標準問法旨在向語言生成器提供標準範本，將標準問法輸入後，機器會自動在後台生成關鍵字，並根據特定的環境、模擬情緒、語境生成不同的問法。設立標準答案也是同理，機器會根據輸入的內容在後台生成答案關鍵字，關鍵字的數量以輸入對話的內容長度相關，對話越長關鍵字數量越多。關鍵字亦可通過人工操作手動添加，評分系統會根據考生的答案篩選關鍵字的數量進行給分。

4. 混合教學模式

教師可將反詐偵防平台的通話錄音轉寫入訓練平台，根據基層警務人員的現實經驗編寫課程教案。充分發揮線上培訓的規模化、碎片化、快捷化優勢，同步開展“線上規模化訓練，線下精英化訓練”的授課模式。二者可相互支持、共同進化：教師可將線上訓練平台統計的高頻率話術片語編入教案，亦可通過開展線下問答、情境交流、組合討論的方式優化反詐培訓課程教學方案。

5. 問答評分設置

相似問答分為相似問法、相似答案和相似關鍵字。相似問答是指系統在不同模擬情緒和語境下的提問方式，相似關鍵字是指和預設關鍵字語義相同或相似的辭彙。相似答案具備和標準答案相同的權重賦值，學員的回答中若是涵蓋了相似關鍵字，在考核評審中仍然可以得分。此外還需要進行敏感詞監測設置，敏感詞是指學員在問答訓練中不能說的詞，主要包括嘲諷、侮辱、煽動性質的辭彙。敏感詞的設置不需要打開題庫進行，只需要在系統配置欄操作即可。

6. 即時更新回饋

系統後台即時顯示線上人數、練習人數、累計學習時長、平均考核得分等信息要素，從執法業務能力、情緒控制力、語言話術技巧、表達準確度、服務規範、文明禮貌 6 個維度進行綜合考量。通過對任務名稱的分類，可以精確查看題目題型正確率、執法人員的話術準確度、異常總人數、異常總次數，用於分析執法人員的知識薄弱點和易錯點。

（二）反詐課程培訓

1. 反詐語庫建設

反詐話術語料根據現有的反詐攔截手段進行制定，這意味着反詐話術要配合反詐攔截手段進行使用。二者以“橫向協同、縱向貫通”為根本原則，以“事前預防 – 事中攔截 – 事後止損”為基本框架。其中，“事前預防”屬於反詐預警部分，“事中攔截”和“事後止損”屬於反詐勸阻部分。事前預防工作能否取得成效，在於民眾的底層認知邏輯是否形成了心理預防效應；而事中和事後的勸阻環節，則需要修改被害人的底層認知，使其認識到自己遭遇了詐騙行為。

研究話術和勸阻對象之間的匹配機理需要結合勸阻對象遭遇的詐騙類型、年齡、性別、職業、生活習慣等基本信息進行綜合考量，這個過程漫長而複雜，需要大量的實踐數據提供回饋。該智能訓練系統在詐騙類型、職業、性別、年齡等層面依次對反詐話術進行分類，並通過關鍵字的多種組合方式進行擴寫，從而實現對話術的靈活搭配運用。

利用執法語言智能訓練系統進行反詐話術的編寫，需要按照實際執法操作的流程，還得進行專業詞庫和日常語料的擴寫，豐富語境和對練場景內容，設定流程話術關鍵字，文本相似度，正則表達，上下文理解，並進行語速檢測，音量檢測及設置相應閾值。進而通過反覆測試，增加相似問題，增加語料拓寫，豐富流程節點，做到同一問題多種問法，模擬實際執法場景，持續優化對練場景和對練題型，豐富執法人員的培訓感受。

該系統目前已被多個公安機關採用，因此反詐話術的回饋數據收集可通過參與訓練的基層公安民警提

供。由基層民警判斷該話術對於相應類型的被害人是否有效，隨後將勸阻結果或者話術評分回饋至訓練系統數據端，從而對這套話術勸阻效果進行統計，以此篩選出針對此類型的被害人成功率最高的一套勸阻話術。

此外，由於系統部署在騰訊雲伺服器，並支持彈性伸縮，足以解決計算資源的橫向 / 水平擴容場景下的問題（Scale-out），即通過增減雲伺服器實例數來動態調整系統的服務能力。因此該系統可以將已收集到的材料重新進行梳理，歸納總結出可視化的流程方案，更新對練話術，並繪製製作符合實際執法場景的流程架構，形成系統對練流程及初步語料庫。

2. 話術能力考核

在完成專業化課程定製和反詐語料擴寫後，系統便有了充足的題庫和語料庫供學員進行訓練，主要的訓練模式分為快問快答和情景對練模式。快問快答訓練分為培訓模式和考核模式。培訓模式支持整句提示、關鍵字提示、無提示。可指定提示方式，教師也可通過後台操作選擇提示方式。考核模式僅支持顯示考核內容提示。在進行快問快答訓練時，系統支持 7 種評分維度：語速檢測、音量檢測、情緒檢測、超時回覆檢測、關鍵字檢測、敏感詞檢測、話術準確度檢測，並且支持啟用 / 禁用評分項，並可調整評分標準值。關鍵字準確率是學員進行執法語言能力考核的評分依據，也是學員對反詐話術掌握情況的最直觀體現。

在快問快答訓練過程中，系統支持增加相關知識點的彈題，適用於系統操作、服務判斷等功能點的考察。在群眾節點支持一鍵生成相似話術，無需人工手動錄入多種話術，實現豐富客戶表述，給學員提供更高擬真度的體驗。系統支持導入對話錄音，利用人聲分割的技術，將說話人分離，形成對話範本，可以一鍵形成對話流程，方便情景流程配置。系統亦可針對已輸入的標準問法支持一鍵生成 AI 推薦的相似問法，無需人工手動收錄多種問法，實現豐富提問形式。執法人員說話內容即時轉寫，培訓模式下，執法人員說完一句話後，系統即時給出評估結果提示。

3. 情景模擬演練

情景對練作為線上培訓系統重要的組成部分，可以模擬實際的預警、勸阻工作中會出現的對話內容。例如在現實中勸阻對象往往情緒激動，他們會和勸阻主體爭辯不休，強調自己沒有受騙，並且排斥勸阻主體所傳遞的信息。情景對練和問答訓練模式不同，快問快答訓練僅僅是對學員基礎話術能力的考核，考驗的是學員對話術的記憶程度。因此快問快答訓練採取的是固定的提問模式，這種訓練模式雖然能利用流水線般的問答範式提高學員對話術的掌握程度，訓練速度快、時間成本低，但是對話的真實感有所欠缺，仍然無法考核學員在複雜情況下對話術的應用能力。

為了進一步提高訓練強度，加強問答訓練的真實感，該執法語言訓練系統推出了情景對練功能。情景對練的底層邏輯如下：確定本輪對話是否為預設打斷位置；若為預設打斷位置，則即時採集學員的對話音頻作為已採集音頻，並對已採集音頻進行檢測；根據已採集音頻的檢測結果確定本輪對話是否滿足預設打斷條件；若滿足預設打斷條件，則停止採集本輪對話中學員後續的對話音頻，直接開啟下一輪對話。由此，可以在學員當前已採集音頻滿足預設打斷條件時，停止繼續採集學員後續的音頻以達到打斷學員繼續作答的效果，增加了學員訓練過程中的真實性和緊張感，可以有效提高學員的心理素質和訓練效果。

一般情況下亦可通過設置數字人模擬問答情緒來決定打斷次數，模擬問答情緒可以讓數字人根據情緒設定生成不同語速、語調的音頻，設置不同的打斷次數，來模擬相關的人類情感。如果情緒設置為憤怒，那麼系統將會提高打斷次數和語速，模擬真實的對話環境；如果情緒設置為悲傷，系統則會針對個別關鍵字反覆生成提問，以模擬人類情緒中躊躇不定的狀態，與此同時系統會檢測考生答案中是否存在安撫情緒等關鍵字，以考察考生的情緒溝通和控場能力。

五、課程意義

（一）提升警察素質

勸阻主體業務素養優化。反詐預警和勸阻工作的根本意義在於重塑被害人的心理認知，恢復其辨認能力，本質上是“反洗腦”的過程，而不是單純的阻止被害人向詐騙分子轉賬。利用執法語言智能訓練系統對執法民警進行訓練，融入反詐溝通話術、專業金融知識和法律條文，可有效利用碎片時間加強民警溝通技巧、話術語言能力，優化其業務素養，使其在執法過程中對專業金融知識、反詐話術知識的運用更加得心應手。

業務工作效能優化。公安執法涉及大量的信息處理工作，包括案件調查、證據收集、嫌疑人審訊等。語言智能化技術可以快速處理大量的語言信息，提高信息處理效率，縮短案件處理周期。通過自動化文本處理和智能輔助工具，可以大幅提高執法部門處理大量執法相關文本和信息的效率，這其中包括法律檔的分類整理、證據的篩選和整理、報告的生成等任務，使執法人員能夠更快速地獲取所需信息並做出相應決策。

語言智能化技術可以幫助公安執法人員更準確地理解和分析語言信息，減少誤解和翻譯錯誤，提高執法品質和精確度。通過案件分析與預測工具，執法人員可以基於數據驅動的分析和預測，制定更科學合理的執法策略。這有助於優化資源配置、提高案件偵破率，提升執法工作的品質和效果。深化推進警務機制和勤務制度改革創新，確保國家政治安全和社會大局持續穩定。

（二）規範執法語言

執法語言標準化（反詐話術語料庫專業化）：利用執法語言智能訓練系統的機器學習和自然語言處理技術，可根據執法情境、詐騙類型、被害人心理特徵，結合心理學、金融學、語言學等專業知識，進行反詐話術語庫的構建，以此編撰標準統一、實用性強、操作性強的執法語言和勸阻話術組合，保障公安民警在執法過程中有法可依、有理可據、有章可循，以合法合規、措辭嚴謹、感染力強的執法語言開展執法活動。

情感分析專業化：了解被害人的心理狀態和心理認知，有助於勸阻人員取得其信任，消除其心理壁壘。執法語言智能訓練系統通過模擬數字人的情感，調整對應的語音、語調、重複次數、打斷次數來實現更好的情感擬真效果，可有效強化公安民警的情感分析能力，優化其話術溝通技巧，使其可以在複雜執法環境下判斷受害人的心理狀況，並選擇合適的話術組合進行預警、勸阻和心理疏導工作。

法律知識普及化：法律智能問答系統可以為勸阻人員提供即時的法律諮詢和指導，並提供相關的法律條文和解釋。這為反詐勸阻工作提供了便捷的法律支持，大幅提高其準確性和專業性。

（三）貼近實戰訓練

執法語言訓練常態化。智能執法語言系統的最大優勢就是縮減了訓練成本和訓練周期，利用自然語言處理（NLP）和人機對話系統（DS）及相關人工智慧技術開展執法語言培訓，使得執法語言訓練碎片化、快捷化、便利化；同時也推動了訓練模式智能化、專業考核標準化。該訓練系統的受眾面廣泛，培訓主體包括一線執法民警、警務輔助人員，還包括警校在校學生。通過科學的課程分類，結合執法情境、案件類型、崗位需求、警種差異進行專業化課程定製，設計出擬真度高、貼近實戰標準的訓練場景，實現執法語言培訓實戰化、常態化。

執法語言考核標準優化。利用深度學習和自注意力機制對龐大的系統數據集、反詐話術集、法律知識、金融學知識進行特徵提取、詞向量賦值、知識圖譜建模，並將最終導出結果結合自然語言理解、自動語音識別、對話管理、自然語言生成、語音合成等 5 個方面進行分析研判，使得執法語言能力、反詐話術能力的考核評分更加人性化。與此同時，該訓練系統可以基於訓練平台的歷史數據和即時信息，進行執法語言需求趨勢預測、風險評估和決策優化，為基層執法人員提供有利的執法建議，提高執法行動的效果，減少執法失誤。

六、結語和展望

加強警察語言訓練，並借助高科技手段縮減訓練周期和成本正是大勢所趨。為了滿足人民群眾對公平公正和安全穩定的新期待、新要求，積極推進中國特色社會主義和諧社會建設，公安民警現場執法語言規範化建設仍需不斷探索和改善。在執法現場根據瞬息萬變的執法環境迅速進行分析，準確決斷採用合適的語言、語速、語調表達的能力，是公安民警應該掌握的基本技能。

針對執法主體的執法語言訓練應當以人為本，以人工智慧助力公安民警執法語言培訓，激發公安民警執法語言活力。隨着智能執法語言使用的執法效率和準確率的提高，警察的工作體驗和個人安全得到了更好的保障。各地公安機關應當聯合各研究機構、高校或高新技術企業進行技術研發，加強對於執法語言智能化的技術支持與科技支撐。加強警察語言訓練可以使執法變為本能反應，加強話術培訓使勸阻過程更加得心應手，進而推進執法規範化建設，改善反詐業務工作，將社會公共安全與秩序的維護落到實處。

《澳門警學》投稿須知

《澳門警學》是在澳門特別行政區政府保安司指導下，由澳門保安部隊和保安部門聯合籌辦，澳門保安部隊高等學校出版的綜合性警學期刊，於 2022 年創刊，每年出版兩期，致力為警界提供交流探討警學理論與實務經驗的平台，在國家安全、犯罪偵查、治安管理、海關執法、懲教監管和消防安全等相關領域分享研究成果。

我們熱切期待專家學者、警界同仁不吝賜稿，文章一經採用，將奉稿酬，聊表謝忱！來稿須從未於其他刊物、網絡及媒體刊登或轉載，倘出現抄襲、洩密或侵害他人知識產權等情況，由來稿者承擔法律責任，本刊概不負責。凡向本刊投稿並經錄用，即視為同意將該作品的發行權、複製權、資訊網絡傳播權、翻譯權、彙編權授予本刊。

本刊在編輯過程中，得對來稿文章進行修改，如不同意，請在來稿時聲明。

來稿者請按以下格式投稿：

一、基本格式

(一) 來稿字數為8,000–12,000字，包括：中文及英文題目、中文及英文摘要(約200字)、中文及英文關鍵詞(三至五個)、作者資料(姓名及其拼音、工作單位、職稱、學歷)。

(二) 內文請統一採用新細明體，繁體字、字體大小12，分段請空兩格。

- 內文一級標題為序號一、
- 內文二級標題為序號(一)
- 內文三級標題為序號1.
- 內文四級標題為序號(1)

(三) 標點用現代漢語標點符號(全形)。

二、註釋體例

(一) 文章註釋以[1]、[2]、[3]順序……上標於文字的右上角，並採用頁下腳註形式。

(二) 文章的註釋格式如下：

1. 中文文獻
   - 【專著】作者姓名：《書名》，出版社，出版年份，頁碼。
   - 【期刊】作者姓名：〈篇名〉，《期刊名稱》，出版年期，頁碼。
   - 【新聞】作者姓名：〈文章題目〉，《報章名稱》，出版日期，版面。
   - 【網絡資源】作者姓名：〈文章題目〉，網站名稱，網址，到訪日期。
2. 外文文獻
   - 【專著】Author, Title of the book, Publisher, Year of publication, Page.
   - 【期刊】Author, “Title of the Article”, Title of the Journal, Volume, Number/Issue, Year, Page.
   - 【新聞】Author, “Title of the Article”, Name of the Newspaper, Date of Issue, Page.
   - 【網絡資源】Author, “Title of the Article”, URL, Date of retrieval.

三、格式說明未詳列之處，請按《學術論文編寫規則》(GB/T 7713.2–2022) 要求編排。

四、本刊聯繫途徑

地址：澳門路環石街澳門保安部隊高等學校《澳門警學》期刊編輯委員會
電郵：esfsm–mag@fsm.gov.mo
電話：(853)2887 1112
傳真：(853)2887 1117

出版：澳門保安部隊高等學校
地址：澳門路環石街
電話：(853) 2887 1112
圖文傳真：(853) 2887 1117
網站：www.fsm.gov.mo/ESFSM
電子郵件地址：esfsm-mag@fsm.gov.mo

印刷：印務局

出版日期：2024 年 9 月

發行量：200 冊

ISSN 2789-9942

澳門特別行政區政府
澳門保安部隊高等學校

地址：澳門路環石街

ISSN 2789-9942

Governo da Região Administrativa Especial de Macau
Escola Superior das Forças de Segurança de Macau

Endereço: Calçada do Quartel, Coloane, Macau